UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	01/10/2017	9542571	11913-US-CNT3 4214-25714	5874

82313 7590 12/21/2016

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

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) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Neil P. Adams, Kitchener, CANADA;
BlackBerry Limited, Waterloo, CANADA;
Michael G. Kirkup, Waterloo, CANADA;
Herbert A. Little, Waterloo, CANADA;
Russell N. Owen, Waterloo, CANADA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	9	6141754		2000-10-31	Choy	
	10	6167521		2000-12-26	Smith, et al.	
	11	6192476	B1	2001-02-20	Gong	
Change(s) applied to document, /J.G./ 8/31/2016	12	6202207	B1	03/2001 ~~2011-03-13~~	Donohue	
	13	6212635	B1	2001-04-03	Reardon	
	14	6216116	B1	2001-04-10	Barkan, et al.	
	15	6233608	B1	2001-05-15	Laursen, et al.	
	16	6480961	B2	2002-11-12	Rajasekharan, et al.	
	17	6487665	B1	2002-11-26	Andrew, et al.	
	18	6513121	B1	2003-01-28	Serkowski	
	19	6922782	B1	2005-07-26	Spyker, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714	5874

82313 7590 11/28/2016

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

EXAMINER	
HESS, DANIEL A	

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
11/28/2016	ELECTRONIC

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

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

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

ConleyRoseReporting@dfw.conleyrose.com

Response to Rule 312 Communication	Application No.	Applicant(s)
	14/715,227	ADAMS ET AL.
	Examiner	Art Unit
	DANIEL HESS	2876

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

1. ☒ The amendment filed on *11/17/2016* under 37 CFR 1.312 has been considered, and has been:

a) ☐ entered.

b) ☒ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.

Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

Attached please find IDS of 11/16/2016, which has been reviewed. The IDS did not change the examiner's view that the claims are allowable.

/DANIEL HESS/
Primary Examiner, Art Unit 2876

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

	1	Brazilian Office Action as Received in Co-pending Application No. PI0317233-3 on September 1, 2016; 5 pages. (No English translation available; Attorney Docket No. 4214-27104)

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DANIEL A HESS/	Date Considered	11/21/2016

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

X The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2016-11-16
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

OK TO ENTER: /D.A.H/

Attorney Docket No. 11913-US-CNT[3]
4214-25714

11/21/2016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: BlackBerry Limited	§	
	§	Group Art Unit: 2876
Application No.: 14/715,227	§	
	§	Examiner: Daniel A. Hess
Filed: May 18, 2015	§	
	§	Confirmation No.: 5874
For: SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES	§	

AMENDMENT UNDER 37 CFR § 1.312

Commissioner:

Please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims that begins on Page 2 of this paper.

Remarks begin on Page 9 of this paper.

Electronic Acknowledgement Receipt

EFS ID:	27542001
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Lesley Forte
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	17-NOV-2016
Filing Date:	18-MAY-2015
Time Stamp:	14:17:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$960
RAM confirmation Number	111816INTEFSW00000510501515
Deposit Account	501515
Authorized User	Lesley Forte

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	11913-US-CNT3_2016-11-17_SUB_IF.pdf	1092525 ea5cb56771daa5da3f2f3d40eedb8bfd12aad2de	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30791 b98a599782bcd2b5ed36d51265bd6e49fa092efb	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1123316		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14715227
Filing Date:	18-May-2015
Title of Invention:	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	J. Robert Brown/Lesley Forte
Attorney Docket Number:	11913-US-CNT3 4214-25714

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	960	960

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**960**

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 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: Use Block 1 for any change of address)

82313 7590 08/17/2016
Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

Note: A certificate of mailing 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 or transmission.

Certificate of Mailing or Transmission
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 Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Lesley Forte	(Depositor's name)
/Lesley/ Forte/	(Signature)
November 17, 2016	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3	5874

TITLE OF INVENTION: SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES 4214-25714

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	11/17/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
HESS, DANIEL A	2876	235-375000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ 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; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

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 Conley Rose, P.C.
2 J. Robert Brown, Jr.
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. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: BlackBerry Limited

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Waterloo, Ontario Canada

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 submitted:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 50-1515 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /J. Robert Brown, Jr./ Date November 17, 2016
Typed or printed name J. Robert Brown, Jr. Registration No. 45,438

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Nintendo Exhibit 1003
Part 1 of 2
Page 0014

REMARKS

The Applicant thanks the Examiner for the Notice of Allowance mailed August 17, 2016. Claim 16 is hereby amended to correct certain informalities in the language of the claim. The amendment does not introduce new matter or alter the scope of the claims. Accordingly, the Applicant respectfully requests entry of the present amendment.

CONCLUSION

The Applicant respectfully submits that the application, in its present form, is in condition for allowance. If the Examiner has any questions or comments or otherwise feels it would be helpful in expediting the application, the Examiner is encouraged to telephone the undersigned at (972) 731-2288. The Applicant intends this communication to be a complete response to the Notice of Allowance mailed August 17, 2016.

The Commissioner is hereby authorized to charge payment of any fee associated with any of the foregoing papers submitted herewith or any fees during the prosecution of the present case to Deposit Account No. 50-1515, Conley Rose, P.C.

Respectfully submitted,

CONLEY ROSE, P.C.

Date: November 17, 2016

/J. Robert Brown, Jr./
J. Robert Brown, Jr.
Reg. No. 45,438

ATTORNEY FOR APPLICANT

5601 Granite Parkway, Suite 500
Plano, Texas 75024
Telephone: (972) 731-2288
Facsimile: (972) 731-2289

Electronic Acknowledgement Receipt

EFS ID:	27541959
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Lesley Forte
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	17-NOV-2016
Filing Date:	18-MAY-2015
Time Stamp:	14:11:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		11913-US-CNT3_2016-11-17_SUB_Amendment_After_Allowance.pdf	51674 cfa5e8e97ea4308bc8318d66a8fa8e9579640adc	yes	9

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment after Notice of Allowance (Rule 312)	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	9
Warnings:			
Information:			
	Total Files Size (in bytes):	51674	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: BlackBerry Limited	§	
	§	Group Art Unit: 2876
Application No.: 14/715,227	§	
	§	Examiner: Daniel A. Hess
Filed: May 18, 2015	§	
	§	Confirmation No.: 5874
For: SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES	§	

AMENDMENT UNDER 37 CFR § 1.312

Commissioner:

Please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims that begins on Page 2 of this paper.

Remarks begin on Page 9 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Previously Presented) A method of application control on an electronic device, the method comprising:

receiving, by the electronic device, owner information from an owner of the electronic device;

receiving, by the electronic device, owner control information that comprises:

a list of applications permitted for installation on the electronic device, and

permissions associated with each permitted application in the list of applications;

storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;

determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and

controlling application access to the local memory based upon the determining.

2. (Original) The method of claim 1, wherein the request to access the local memory comprises a request to erase data from the local memory.

3. (Original) The method of claim 1, wherein the request to access the local memory comprises a request to read data from the local memory.

4. (Canceled)

5. (Previously Presented) The method of claim 1, further comprising restricting modification of the owner control information after the owner control information has been stored in the protected data store.

6. (Previously Presented) The method of claim 1, wherein the owner control information includes an authorization record and an application identifier for each of the applications, and the owner control information is provided by an external source through a wireless communication channel.

7. (Previously Presented) The method of claim 6, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

8. (Previously Presented) The method of claim 1, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

Nintendo Exhibit 1003
Part 1 of 2
Page 0020

9. (Original) The method of claim 1, wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device, the method further comprising:

receiving requests to access the local memory from a plurality of applications operating on the electronic device;

determining whether access to the local memory is allowed to be performed by their respective applications based upon the stored authorization records and the application identifiers that are respectively associated with the plurality of applications; and

controlling access by the plurality of applications to local memory based upon whether access to the local memory is allowed.

10. (Original) The method of claim 9, wherein a group containing two or more of the applications is associated with one of the authorization records.

11. (Canceled)

Nintendo Exhibit 1003
Part 1 of 2
Page 0021

12. (Previously Presented) A device, comprising:

a memory; and

a processor coupled with the memory and configured by instructions stored in the memory to:

receive owner information from an owner of the device;

receive owner control information that comprises:

a list of applications permitted for installation on the device, and

permissions associated with each permitted application in the list of applications;

store the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receive, from an application operating on the electronic device, a request to access local memory on the electronic device;

determine whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and

control application access to the local memory based upon the determining.

13. (Original) The device of claim 12, wherein the request to access the local memory comprises a request to erase data from the local memory.

Nintendo Exhibit 1003
Part 1 of 2
Page 0022

14. (Original) The device of claim 12, wherein the request to access the local memory comprises a request to read data from the local memory.

15. (Canceled)

16. (Currently Amended) The device of claim 12, wherein the processor is further configured to restrict~~further comprising restricting~~ modification of the owner control information after the owner control information has been stored on the electronic device.

17. (Previously Presented) The device of claim 12, wherein the owner control information includes an authorization record and an application identifier for each of the applications, and wherein the owner control information is provided by an external source through a wireless communication channel.

18. (Previously Presented) The device of claim 17, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

19. (Previously Presented) The device of claim 12, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

Nintendo Exhibit 1003
Part 1 of 2
Page 0023

20. (Previously Presented) A non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the operations of:

receiving owner information from an owner of an electronic device;

receiving owner control information that comprises:

a list of applications permitted for installation on the electronic device, and

permissions associated with each permitted application in the list of applications;

storing the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receiving, from an application operating on the electronic device, a request to access local memory on the electronic device;

determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and

controlling application access to the local memory based upon the determining.

21. (Previously Presented) The non-transitory computer-readable medium of claim 20, wherein the owner control information includes an authentication record and an identifier for each application allowed to be executed on the electronic device.

Nintendo Exhibit 1003
Part 1 of 2
Page 0024

22. (Previously Presented) The non-transitory computer-readable medium of claim 20, wherein the request to access the local memory comprises a request to erase data from the local memory.

23. (Previously Presented) The non-transitory computer-readable medium of claim 20, wherein the request to access the local memory comprises a request to read data from the local memory.

Electronic Patent Application Fee Transmittal

Application Number:	14715227
Filing Date:	18-May-2015
Title of Invention:	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	J. Robert Brown/Rami Law
Attorney Docket Number:	11913-US-CNT3 4214-25714

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14715227
	Filing Date	2015-05-18
	First Named Inventor	Neil P. Adams
	Art Unit	2876
	Examiner Name	Daniel A. Hess
	Attorney Docket Number	11913-US-CNT3 4214-25714

	1	Brazilian Office Action as Received in Co-pending Application No. PI0317233-3 on September 1, 2016; 5 pages. (No English translation available; Attorney Docket No. 4214-27104)

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2016-11-16
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	27526692
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Rami Law
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	16-NOV-2016
Filing Date:	18-MAY-2015
Time Stamp:	16:57:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$180
RAM confirmation Number	111716INTEFSW00003406501515
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	11913-US-CNT3_2016-11-16_IDS.pdf	614695 ab6546805d9343ae613079cb80efc03579f9d6bb	no	4
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Other Reference-Patent/App/Search documents	BRExamReport_27104_090116.pdf	154105 29289d42f0e8180603ada12259ed9018ae2a1b22	no	5
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30885 fb2f080d8cf04b72736e32cf546ebb8f82889a08	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	799685		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714	5874

82313 7590 09/16/2016

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

EXAMINER	
HESS, DANIEL A	

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
09/16/2016	ELECTRONIC

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

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

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

ConleyRoseReporting@dfw.conleyrose.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
14/715,227	18 May, 2015	ADAMS ET AL.	11913-US-CNT3 4214-25714

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

EXAMINER	
DANIEL HESS	
ART UNIT	PAPER
2876	20160911

DATE MAILED:

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

Commissioner for Patents

Attached please find IDS of 9/8/2016, which has been considered. No response to this notice is needed from the applicant.

/DANIEL HESS/
Primary Examiner, Art Unit 2876

PTO-90C (Rev.04-03)

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2003201905	AU	A1	2003-07-24	NTT Docomo, Inc.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

	1	European Intention to Grant; Application No. 05739066.8; July 6, 2016; 70 pages. (4214-25708)

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DANIEL A HESS/	Date Considered	09/11/2016

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

X The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2016-09-08
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

Electronic Acknowledgement Receipt

EFS ID:	26867450
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Rami Law
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	08-SEP-2016
Filing Date:	18-MAY-2015
Time Stamp:	14:34:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	889
Deposit Account	501515
Authorized User	Law, Rami

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	11913-US-CNT3_2016-09-08_IDS.pdf	614700 50768cb01864308d9163575aa59c286029f91659	no	4
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Foreign Reference	AU2003201905A1.pdf	7052819 a2c112c47bff58ce54c2cafb549b92868b464626	no	59
Warnings:					
Information:					
3	Other Reference-Patent/App/Search documents	EPNOA_25708_070616.pdf	11334203 b09d4d671cdcbb5361822032743baeb4d7de1f3d	no	70
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30884 007a8704b6a3bf5545f9e75b481bbf684c9258e6	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	19032606		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Electronic Patent Application Fee Transmittal

Application Number:	14715227
Filing Date:	18-May-2015
Title of Invention:	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	J. Robert Brown/Rami Law
Attorney Docket Number:	11913-US-CNT3 4214-25714

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2003201905	AU	A1	2003-07-24	NTT Docomo, Inc.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14715227
	Filing Date	2015-05-18
	First Named Inventor	Neil P. Adams
	Art Unit	2876
	Examiner Name	Daniel A. Hess
	Attorney Docket Number	11913-US-CNT3 4214-25714

	1	European Intention to Grant; Application No. 05739066.8; July 6, 2016; 70 pages. (4214-25708)

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2016-09-08
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(11) Application No. AU 2003201905 A1

(19) AUSTRALIAN PATENT OFFICE

(54) Title
CONTENT DELIVERY METHOD AND CONTENT DELIVERY SYSTEM

(51)[6] International Patent Classification(s)
G06F 001/00 G06F 009/06

(21) Application No: 2003201905 (22) Application Date: 2003.01.07

(87) WIPO No: WO03/058411

(30) Priority Data

(31) Number	(32) Date	(33) Country
2002-1843	2002.01.08	JP

7

(43) Publication Date : 2003.07.24

(43) Publication Journal Date : 2003.09.04

(71) Applicant(s)
NTT DOCOMO, INC.

(72) Inventor(s)
KAWABATA, Hiroshi; KONDO, Takashi; YAMADA, Kazuhiro; WATANABE, Nobuyuki ; TSUDA, Masayuki; KAMIYA, Dai; ASAI, Mao; MIURA, Fumiaki; WASHIO, Satoshi ; TOMIOKA, Atsuki

Nintendo Exhibit 1003
Part 1 of 2
Page 0050

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年7 月17 日 (17.07.2003)

PCT

(10) 国際公開番号
WO 03/058411 A1

(51) 国際特許分類[7]: G06F 1/00, 9/06

(21) 国際出願番号: PCT/JP03/00035

(22) 国際出願日: 2003 年1 月7 日 (07.01.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-1843 2002 年1 月8 日 (08.01.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目11番1号 Tokyo (JP).

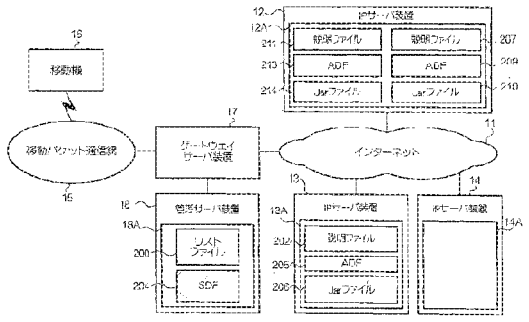
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 山田 和宏 (YAMADA,Kazuhiro) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 渡邊 信之 (WATANABE,Nobuyuki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 津田 雅之 (TSUDA,Masayuki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 神谷 大 (KAMIYA,Dai) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 浅井 真生 (ASAI,Mao) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 三浦 史光 (MIURA,Fumiaki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 鷲尾 諭 (WASHIO,Satoshi) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 富岡 淳樹 (TOMIOKA,Atsuki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二

[続葉有]

(54) Title: CONTENT DELIVERY METHOD AND CONTENT DELIVERY SYSTEM

(54) 発明の名称: コンテンツ配信方法およびコンテンツ配信システム



16...MOBILE APPARATUS
15...MOBILE PACKET COMMUNICATION NETWORK
17...GATEWAY SERVER APPARATUS
18...MANAGEMENT SERVER APPARATUS
200...LIST FILE
12...IP SERVER APPARATUS
211...EXPLANATION FILE
207...EXPLANATION FILE
214...Jar FILE
210...Jar FILE
11...INTERNET
13...IP SERVER APPARATUS
202...EXPLANATION FILE
206...Jar FILE
14...IP SERVER APPARATUS

(57) Abstract: A mobile apparatus (16) capable of activating Java-AP software receives SDF (Security Description File)(204) from a management server apparatus (18) managed by a reliable organization (a communication business entity managing a mobile packet communication network 15); obtains ADF (205) from an IP server apparatus (13) by use of a URL included in the SDF; obtains a Jar file (206) from the IP server apparatus (13) by use of the ADF (205); and installs into itself Java-AP software including these files. The Java-AP, which is realized by activating the Java-AP software, operates within the range of the right represented by policy information included in the SDF (204).

[続葉有]

WO 03/058411 A1

丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 川端博史 (KAWABATA,Hiroshi) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 近藤 隆 (KONDO,Takashi) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP).

(74) 代理人: 川崎 研二 (KAWASAKI,Kenji); 〒103-0027 東京都 中央区 日本橋一丁目２番１０号 東洋ビルディング７階 朝日特許事務所 Tokyo (JP).

(81) 指定国 (国内): AU, BR, CA, CN, ID, IN, KR, NO, NZ, PH, PL, SG, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

添付公開書類:
国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

Ｊａｖａ－ＡＰソフトウェアを起動することができる移動機１６が、信頼できる機関（移動パケット通信網１５を管理する通信事業者）が管理する管理サーバ装置１８からＳＤＦ（セキュリティ記述ファイル）２０４を受信し、このＳＤＦに内包されているＵＲＬを用いてＩＰサーバ装置１３からＡＤＦ２０５を取得し、このＡＤＦ２０５を用いてＩＰサーバ装置１３からＪａｒファイル２０６を取得し、これらのファイルを内包するＪａｖａ－ＡＰソフトウェアを自身にインストールする。このＪａｖａ－ＡＰソフトウェアを起動することで実現されるＪａｖａ－ＡＰは、ＳＤＦ２０４に内包されているポリシー情報で表される権限の範囲内で動作する。

VERIFICATION STATEMENT OF TRANSLATION

Re: Australian Patent Application
Based on International Application No. PCT/JP03/00035

I, Takashi MATSUMOTO, a Japanese citizen of 7th Floor, Toyo Building, 2-10, Nihonbashi 1-chome, Chuo-ku, Tokyo 103-0027 Japan, hereby declare that I am conversant with the document attached and certify that to the best of my knowledge and belief the attached document is a true and correct translation of International Application No. PCT/JP03/00035.

Signature: T. Matsumoto
Takashi MATSUMOTO

Date: June 18, 2004

SPECIFICATION

CONTENTS TRANSMISSION METHOD AND CONTENTS TRANSMISSION SYSTEM

Technical Field

The present invention relates to transmitting application software to terminal units.

Background Art

Mobile units equipped with a function of executing Java-AP (Java Application) software by carrying out a program written in accordance with Java (trademark registered) programming language, and downloaded via a network are in widespread use.

Java-AP software includes a Jar (Java Archive) file and an ADF (Application Descriptor File). The Jar file contains a program, which provides a user with certain Java-AP. The ADF is dependent upon the Jar file, and contains, for instance, URL showing where a Jar file is stored (hereinafter, referred to as package URL), the size of a Jar file, the most recent date when a Jar file is changed and other necessary information.

A mobile unit downloads the relevant software to the desired Java-AP by following the process described below. First, the mobile unit obtains an ADF pertaining to the desired Java-AP from a server unit, which constitutes WWW (World Wide Web).

The mobile unit, which obtains an ADF checks the content of the ADF, and determines whether the Jar file pertaining to the desired Java-AP can be installed in the mobile unit. When the mobile unit determines that Java-AP software can be installed, the mobile unit obtains from a server unit, which constitutes WWW a Jar file by using package URL contained

in the ADF. The process of downloading Java-AP software is complete when the Jar file is obtained. Hereinafter, in the mobile unit, installation of the downloaded Java-AP software is carried out, and the Java-AP software can be activated when required.

Incidentally, when the Java-AP software is installed in a mobile unit the activation of Java-AP is subject to greater restriction than the activation of functions that are native to the mobile unit, such as a communication application function. The activation of a Java-AP is restricted in that it is unable to access certain data contained in a mobile unit, such as telephone numbers for example. By imposing strict restrictions in this manner, leakage or falsification of confidential data contained in a mobile unit, occurring due to malfunctioning Java-AP or caused intentionally, can be prevented.

However, imposing the above-mentioned restriction on all Java-AP uniformly does not adequately meet the needs of a user of a mobile unit or an IP (information provider). For instance, some users seem to feel that Java-AP could be allowed to refer to some of the private information stored in a mobile unit as long as security is guaranteed. Also, some IPs wish to provide Java-AP, which uses some of the private information stored in a mobile unit, or some of the functions a mobile unit is equipped with.

To fulfill these requirements, a system in which a trustworthy organization such as a communication provider providing a communication service to users of mobile units working as an authority, is entrusted with the responsibility of authorizing Java-AP to operate with greater flexibility. Mobile units using Java-AP are notified by the authorization of the operational rules set for Java-AP, and the mobile units can restrict the operation of Java-AP on the basis of the prescribed rules. In this system, only a trustworthy organization should be entrusted to administer the

authorization of a more flexible operation of Java-AP.

When the above-mentioned system is applied to the downloading process of Java-AP software, information showing the authorization in an ADF or a Jar file must be included. Since a Jar file is updated by an IP as required, and it is appropriate for an IP to own a Jar file, it is appropriate for the corresponding ADF to contain information on the validity of the authorization.

However, since the content of an ADF is dependent upon a Jar file, an ADF owned by a trustworthy organization needs to be updated once an IP updates a Jar file. Also, updating an ADF becomes necessary at times even without the updating of a Jar file, as in the instance where access to a certain Jar file gets deluged, and the Jar file is moved to another server unit in the IP. In this instance, since the location where the Jar file is stored is changed, a package URL contained in the ADF needs to be changed. However, since the ADF is administered by a trustworthy organization and excludes the involvement of other agents, the updating operation of an ADF could become a very busy one.

Disclosure of Invention

The present invention was developed to overcome the stated problems of the conventional art, and its object is to provide a transmission method and a transmission system for transmitting without restricting the freedom of an IP to a terminal unit which allows an application to operate in accordance with an authorization, software for achieving an application which is transmitted by transmitting a plurality of files which are dependent upon each other.

To solve the above-mentioned problem of the conventional art, the present invention provides a transmission method comprising: a process for transmitting an authorization file in a communication system in which an

originator originates a request including information showing a storage of a file and the file is transmitted in response to the request, the process for transmitting including transmitting a security descriptive file as the authorization file from an administering server unit storing the security descriptive file through a secure link to a terminal unit, the security descriptive file containing first identification information and authorization information, the first identification information showing a storage location of an application descriptive file, the application descriptive file having information dependent upon an entity file, which includes software for executing an application, along with information showing a storage location of the entity file, the authorization information of the security descriptive file indicating an allowable range of an operation of the application which is executed in accordance with the software, the terminal unit executing operation of the application within a range shown by the authorization information; a dependent information obtaining process for the terminal unit to obtain, by using the first identification information contained in the security descriptive file transmitted from the communication system in the authorization transmission process, the application descriptive file from one or a plurality of server units in which the application descriptive file is stored; and a program obtaining process for the terminal unit to obtain the entity file from the communication system by using the application descriptive file obtained in the dependent information obtaining process.

By this transmission method, the terminal unit obtains before obtaining the application descriptive file and the entity file corresponding to the application, the security descriptive file, which is transmitted by the communication system after security has been assured. In the security descriptive file, the authorization given to the application is denoted, and in the terminal unit, the application corresponding to the security descriptive

file is allowed to operate in accordance with the authorization denoted by the obtained security descriptive file.

Also, the present invention provides a transmission system comprising: a communication system for returning, when a stored location of a file is notified, the file which comprises one or a plurality of server units in which an entity file containing software for achieving an application and an application descriptive file which has a content dependent upon the entity file showing a stored location of the entity file, and an administering server unit in which a security descriptive file containing a first identification information showing a stored location of the application descriptive file and authorization information showing authorization given to an application which is achieved when a terminal unit executes the software is stored; and a terminal unit which approves operation of an application in accordance with authorization given to the application, wherein the administering server unit transmits the security descriptive file to the terminal unit by assuring security, and wherein the terminal unit obtains the application descriptive file by using the first identification information contained in the security descriptive file transmitted by the communication system, and the entity file from the communication system by using the application descriptive file.

By this transmission system, the terminal unit, before obtaining the application descriptive file and the entity file corresponding to the application, obtains the security descriptive file transmitted by the transmission system after security has been assured. The authorization given to the application is denoted in the security descriptive file, and in the terminal unit, the application corresponding to the security descriptive file is allowed to operate in accordance with the permission of the authorization denoted by the obtained security descriptive file.

Brief Description of Drawings

Fig. 1 is a block diagram showing the configuration of the transmission system of one embodiment for executing the present invention.

Fig. 2 is a conceptual figure showing data configuration of an ADF inherent to the transmission system.

Fig. 3 is a block diagram showing the configuration of mobile unit 16 constituting the transmission system.

Fig. 4 is a conceptual figure showing the functional configuration of mobile unit 16.

Fig. 5 is a flowchart showing the process of mobile unit 16 for downloading and installing Java-AP software.

Fig. 6 is a conceptual figure showing data configuration of an SDF stored in administering server unit 18 in the transmission system.

Fig. 7 is a conceptual figure showing the content of policy information contained in the SDF.

Fig. 8 is a block diagram for explaining the operation of the transmission system.

Fig. 9 is a diagram showing a list page transmitted in the transmission system.

Fig. 10 is a diagram showing the content of an explanatory file stored in IP server unit 12 constituting the transmission system.

Fig. 11 is a diagram showing an explanatory page transmitted in the transmission system.

Fig. 12 is a diagram showing the content of an explanatory file stored in IP server unit 12.

Fig. 13 is a diagram showing an explanatory page transmitted in the transmission system.

Fig. 14 is a diagram showing the content of an explanatory file

stored in IP server unit 13 constituting the transmission system.

Fig. 15 is a diagram showing an explanatory page transmitted in the transmission system.

Fig. 16 is a sequence diagram for explaining the operation of the transmission system.

Fig. 17 is a sequence diagram for explaining the operation of the transmission system.

Fig. 18 is a sequence diagram for explaining the operation of the transmission system.

Fig. 19 is a block diagram for explaining another operation of the transmission system.

Fig. 20 is a sequence diagram for explaining another operation of the transmission system.

Best Mode of Carrying out the Invention

Hereinafter, by referring to figures, a transmission system, which is one mode of the present invention is explained. In figures, identical codes are given to common portions.

(1) Configuration

As shown in Fig. 1, in the transmission system, IP server units 12 to 14 are connected to Internet 11. IP server unit 12 is administered by the first IP (Internet Provider), and IP server units 13 and 14 are administered by the second IP, which differs from the first IP. IP server units 12 to 14 constitute WWW, and each is equipped with similar hardware and functions to those of a general WWW server unit. Mobile packet communication network 15 is a network a communication provider uses to provide a mobile packet communication service. Mobile unit 16 can perform radio packet communication with mobile packet communication network 15. Gateway server unit 17 is administered by an identical

communication provider to that of mobile packet communication network 15. Gateway server unit 17 is a unit for connecting mobile packet communication network 15 and Internet 11, and has similar configuration to that of a general gateway server unit. Administering server unit 18 is connected to gateway server unit 17 by an exclusive line. Administering server unit 18 also constitutes WWW, and has similar hardware and a function to those of a general WWW unit. Gateway server unit 17 performs packet communication between mobile packet communication network 15 and Internet 11, packet communication between administering server unit 18 and mobile packet communication network 15, and packet communication between administering server unit 18 and Internet 11. Mobile unit 16, by using the relaying function, is able to perform packet communication with IP server units 12 to 14 via mobile packet communication network 15 and Internet 11. Several mobile units exist in the actual transmission system, but only one mobile unit 16 is shown to avoid complicating the figures. For the same reason, only IP server units 12 to 14 are shown.

In the transmission system, mobile unit 16 is capable of receiving Java-AP software from the desired site on Internet 11. Software which mobile unit 16 is capable of receiving is distinguished between the one pertaining to a trusted Java-AP and the one pertaining to a non-trusted Java-AP. A trusted Java-AP software is one which the communication provider administering mobile packet communication network 15 guarantees authenticity of on the basis of the contract with IP administering IP server units 12 to 14. A non-trusted Java-AP software is any Java-AP software other than a trusted Java-AP software.

Administering server unit 18 stores each SDF (Security Descriptive File) pertaining to each trusted Java-AP software, which is transmitted in the transmission system. SDF is a file, which is produced

by the communication provider administering mobile packet communication network 15, and is the file necessary for downloading into a mobile unit the Java-AP software, which uses trusted API (APplication Interface) of the mobile unit. An explanation of trusted API will follow later. As shown in Fig.6, an SDF contains an APID for detecting trusted Java-AP software, policy information, ADF-URL showing the location where an ADF corresponding to the Java-AP software is stored, and public key CA (Certifying Agent) gives to IP which provides the Java-AP software. Policy information is the information showing restriction on the operation of Java-AP. Policy information and the restriction on Java-AP's operation carried out on the basis of the policy information will be explained in detail afterwards.

In the present embodiment, when a trusted Java-AP software is transmitted to mobile unit 16 by one of IP server units 12 to 14, an SDF corresponding to the trusted Java-AP software is transmitted to mobile unit 16 by administering server unit 18 in response to the request from mobile unit 16. In mobile unit 16, when a trusted Java-AP software is executed, restriction on the trusted Java-AP's operation is carried out on the basis of the SDF corresponding to the trusted Java-AP. This is one characteristic of the present embodiment. As shown in Fig.1, transmission of the SDF is carried out via mobile packet communication network 15, and administering server unit 18 and gateway server unit 17 are connected by an exclusive line. Also, for transmission, the SDF is encrypted.

Hereinafter, with regard to relevance to the characteristics, the configuration of each element of the transmission system will be explained.

IP server units 12, 13 and 14 are equipped with fixed memory 12A, 13A and 14A respectively.

Fixed memory 12A, 13A and 14A are fixed memories such as a hard disc, and store Java-AP software constituting Jar files and ADF, and

explanatory files on the content of Java-AP software for users of mobile units.

Each Java-AP software stored in fixed memory 12A, 13A and 14A might be either trusted Java-AP software or non-trusted Java AP software. Whether Java-AP is a trusted Java-AP or a non-trusted Java-AP, in each ADF of Java-AP software, information such as a package URL showing the location where a Jar file in WWW is stored, information showing the size of the Jar file, and information showing the date of the most recent update are written. Such information is generally known as items to be written in the ADF of a Java-AP software. Also, the ADF of a trusted Java-AP software, as shown in Fig.2, contains an APID of the trusted Java-AP and the hash value of the Jar file besides the generally known information. Furthermore, the ADF of a trusted Java-AP software is encrypted by a secret key which CA gives to an IP which provides the software.

Also, the explanatory file is a text file written in accordance with HTML. A mobile unit, when a certain Java-AP software is downloaded, needs to download beforehand the explanatory file corresponding to the Java-AP software. The explanatory file contains information for forming UI (User Interface) for receiving from the user the command for downloading Java-AP software. Mobile unit 16 displays the UI screen in accordance with the information. The user can carry out the operation on mobile unit 16 for specifying the object showing the desired Java-AP on the UI screen. The explanatory file is written for the object specified by the user in this manner so as to correspond to the URL showing where in WWW the SDF (ADF if SDF does not exist) corresponding to Java-AP software which is the object for downloading is located.

Each of IP server units 12 to 14 is equipped with the function of producing and updating each of the above-mentioned files in accordance

with the command of an IP.

Administering server unit 18 is equipped with fixed memory 18A such as a hard disc. Administering server unit 18 establishes a TCP connection with the party. When administering server unit 18 receives a request message which uses the GET method of HTTP from the party via a TCP connection, administering server unit 18 reads out the file identified by the URL specified by the GET method from fixed memory 18A, and returns a response message of HTTP containing the file, and severs the connection.

Also, in the above-mentioned fixed memory 18A are stored, list file 200 for introducing to the user of mobile unit 16 downloadable Java-AP software, and respective SDF corresponding to each Java-AP software which is listed in list file 200.

List file 200, as SDF, is the file produced by the communication provider in accordance with the contract signed by each IP which administers IP server units 12 to 14, and the communication provider which administers administering server unit 18. List file 200 is a text file written in accordance with HTML. As already explained, the mobile unit needs to obtain the explanatory file containing a URL of an SDF to download the SDF of certain Java-AP software. Mobile unit 16 can obtain the explanatory file directly by accessing the IP server unit in which the explanatory file is stored. However, in the present embodiment, mobile unit 16 can obtain the explanatory file of the desired Java-AP software also by the following process as opposed to the above-mentioned direct method. First, mobile unit 16, by accessing administering server unit 18, obtains list file 200, and displays the UI screen accordingly. The user can carry out the operation on mobile unit 16 to specify the object showing the desired Java-AP on the UI screen. List file 200 matches the object specified by the user to a URL showing the location of the

explanatory file of Java-AP software in WWW which is the object of downloading. Mobile unit 16, by using the URL obtained via list file 200, obtains the explanatory file from the IP server unit.

Mobile unit 16 consists of, as shown in Fig.3, OS (Operating System) software; ROM 16A in which Java-AP environment software for establishing the environment for executing the Java-AP, and several types of native AP software are stored; CPU 16B which is connected to ROM 16A for reading out a program from ROM 16A and executing the program; displaying unit 16C which is connected to CPU 16B; fixed memory 16D; RAM 16E; communication unit 16F; and operation unit 16G.

Displaying unit 16C has, for instance, a liquid crystal displaying panel, and displays data provided by CPU 16B as an image. Fixed memory 16D is, for instance, SRAM or EEPROM, and data is read and written by CPU 16B. Fixed memory 16D is used to store Java-AP software (ADF and Jar) downloaded from a server unit (hereinafter, referred to as a Web server unit) constituting WWW, and an SDF.

Communication unit 16F performs radio packet communication with mobile packet communication network 15, and relays packets between CPU 16B and mobile packet communication network 15. Also, communication unit 16F is equipped with CODEC, a microphone, a speaker and so forth for communication besides an antenna or a radio transmission and reception unit. Hence, mobile unit 16, by communication unit 16F, can perform communication by circuit switching via a mobile communication network (not shown). Operation unit 16G is equipped with an operation controller, and provides CPU 16B a signal in accordance with the operation carried out by the operation controller.

As the switch (not shown) is turned on, CPU 16B reads out the program contained in OS software from ROM 16A, and executes with RAM 16E as a work area. As a result, functions for providing UI and so

forth are executed in CPU 16B. In other words, CPU 16B activates OS software, and executes OS of Fig.4 in mobile unit 16. OS identifies the command of the user on the basis of the signal provided by operation unit 16G and the status of UI, and executes the process in accordance with the command.

When the command of the user requests activation of communication software, which is native AP software, OS activates the communication software, and executes communication AP in mobile unit 16. By using communication AP, the user can communicate with the party.

When the command of the user requests the activation of telephone directory AP, which is native AP software, OS activates the telephone directory software, and executes telephone directory AP in mobile unit 16. By using telephone directory AP, the user can refer to, use, and change the content of the telephone directory (hereinafter, referred to as telephone directory data) stored in fixed memory 16D.

When the command of the user requests the activation of Web browser software, which is native AP software, OS activates Web browser software, and executes the Web browser in mobile unit 16. Also, the Web browser provides UI. Then, as the user gives the command by operating operation unit 16G, the Web browser identifies the command of the user on the basis of the status of UI and the signal provided by operation unit 16G, and executes the process in accordance with the command. For instance, when the command is for obtaining the specified file from WWW, a TCP connection is established by operating communication unit 16F with the Web server unit in which the file is stored, a request message of HTTP using the GET method is transmitted by URL showing the specified location, a response message corresponding to the request message is received, and the connection is severed. Furthermore, the Web browser

interprets the file contained in the received response message in accordance with HTML, produces UI containing the Web page, and provides the user. Also, when a user sends a command for downloading Java-AP software, the command is notified to JAM (Java Application Manager). Specifically, in a Web page, either by clicking or pressing, when an anchor tag to which the object tag is specified is designated, the Web browser extracts URL which is specified as data property of the object tag, and notifies JAM that downloading of Java-AP software by URL is requested.

When the command of the user requests the activation of JAM software, which is native AP software, OS activates JAM software, and executes JAM in mobile unit 16. JAM shows to the user a list of Java-AP software installed in mobile unit 16, and activates the Java-AP software specified by the user. Specifically, when the command of the user to JAM requests the activation of Java-AP software, Java-AP environment software is activated, and Java-AP environment is executed in mobile unit 16. Then, the specified Java-AP software is activated, and Java-AP is executed in Java-AP environment. Java-AP environment contains KVM, which is a lightweight Java Virtual Machine appropriate to a cellular terminal, and API provided for Java-AP. API provided for Java-AP is divided into trusted API which only Java-AP whose trustworthiness is guaranteed by the communication provider on the basis of the contract with the IP (hereinafter, referred to as trusted AP) is allowed to use, and non-trusted API which any Java-AP is allowed to use.

(2) Operation

Hereinafter, the operation of the present embodiment is explained. JAM, when a command for requesting the downloading of Java-AP is notified by the Web browser, carries out the process for downloading and installing Java-AP software into mobile unit 16. The flow of the process is shown in Fig. 5. In Fig.5, the process of mobile unit 16 for obtaining

the explanatory file is omitted. Since some different modes exist for the process of obtaining the explanatory file, the process will be later explained with some specific examples of the operation. As shown in Fig.5, JAM first determines whether Java-AP software, which is about to be downloaded, is trusted Java-AP software (Step S11). Specifically, when mobile unit 16 obtains the explanatory file, the Web browser provides the user UI corresponding to the explanatory file, and receives the command for downloading Java-AP software from the user. The Web browser notifies JAM of URL of the Java-AP software specified by the user. JAM refers to the file name at the end of the URL notified by the Web browser, and determines that the software is trusted Java-AP software if the extension of the file is "sdf", and non-trusted Java-AP software if the extension of the file is not "sdf." When the Java-AP software, which is about to be downloaded, is determined as trusted Java-AP software, the downloading and installation processes identical to the conventional processes are carried out (Step S12).

When the Java-AP software, which is about to be downloaded, is determined as trusted Java-AP software, JAM obtains the SDF corresponding to the software from administering server unit 18 (Step S13). In other words, JAM establishes the TCP connection with administering server unit 18, produces and transmits via the TCP connection a request message requesting administering server unit 18 for transmission of the SDF stored in the location shown by URL notified by the Web browser, receives the response message to the request message, and severs the above-mentioned connection.

Then, JAM extracts APID, ADF-URL, and the public key from SDF contained in the response message, and writes SDF into fixed memory 16D.

Next, JAM obtains ADF (Step S14). Specifically, JAM

establishes the TCP connection with the Web server unit in which ADF identified by ADF-URL extracted from SDF is stored, produces and transmits a request message for requesting transmission of ADF, receives a response message to the request message, and severs the TCP connection.

As already explained, an ADF corresponding to trusted Java-AP software, contains the hash values of an APID and a Jar file, and further signed (encrypted) by the secret key CA gives to the IP which provides the trusted Java-AP software. Then, JAM checks (decodes) the signature of the ADF contained in the response message by using the public key extracted from the SDF, and determines the authenticity of the ADF (Step S15).

When an ADF is determined to be authentic, the JAM compares the APID extracted from an SDF to an APID contained in the ADF, and determines whether these APIDs match (Step S16). When these APIDs are determined to match, JAM determines whether the trusted Java-AP software can be installed in mobile unit 16 on the basis of the content of the ADF (Step S17). The basis of determination is identical to the conventional basis.

When installation is determined to be possible, JAM obtains the Jar file. Specifically, JAM writes the ADF into mobile unit 16, and extracts the hash value and package URL from the ADF. Furthermore, JAM establishes the TCP connection with the Web server unit in which the Jar file identified by package URL is stored, produces and transmits a request message for requesting transmission of the Jar file, receives the response message to the request message, and severs the TCP connection (Step S18).

Furthermore, JAM calculates the hash value to the obtained Jar file (Step S19). Any hash function can be used to calculate the hash value, but the hash value used by the mobile unit and the hash value the IP uses

for calculating the hash value contained in the ADF must be identical.

JAM compares the hash value calculated by JAM to the hash value extracted from the ADF (Step S20), writes the obtained Jar file into administering server unit 18 when these hash values match, carries out several kinds of processes pertaining to installation of trusted Java-AP software (Step S21), and notifies the user that installation is successful (Step S22).

When an ADF is determined not to be authentic, when an APID of an SDF and an APID of an ADF do not match, when the Java-AP software which is about to be installed is determined not to be installable, and when the calculated hash value and the hash value of an ADF do not match, the JAM notifies the user that installation has failed, and returns the status of mobile unit 16 to the status that exists before the acquisition of the SDF starts.

Also, JAM supervises the operation of Java-AP, and restricts the use of the trusted API. The restriction is carried out in accordance with policy information in SDF stored in fixed memory 16D. Policy information in SDF, for instance, is the content conceptually shown in Fig. 7. In the policy information shown in Fig.7, the use of the necessary trusted API "getPhoneList()" for referring to telephone number directory data, and the necessary trusted API "getMsStatus()" for obtaining the status of the mobile unit stored in the mobile unit are allowed, and the use of the necessary trusted API for referring to history data of transmission and reception "getCallHistory()" stored in the mobile unit is forbidden.

(3) Specific Operation

Next, the operation of the above-mentioned system is explained.

In the operation explained below, establishment of the TCP connection and severing operation are general operations of HTTP; therefore, the explanation is omitted. Also, the above-mentioned

operations carried out by OS, the Web browser, JAM, Java-AP, native AP and so forth are operations of mobile unit 16; therefore, in the following explanation, the main unit which carries out the operation is mobile unit 16.

In the operation explained hereinafter, the following case is the presupposition. First, as shown in Fig. 8, in fixed memory 18A of administering server unit 18, are stored list file 200 and SDF 204. At this stage, list file 200 is written to provide list page 201 shown in Fig.9 when interpreted and executed by mobile unit 16. Also, list file 200 is written, when option 201A constituting list page 201 is specified either by being clicked or pressed, to produce a request message containing URL of explanatory file 202 ("http://www.main.bbb.co.jp/ghi.html") as a parameter of the GET method. Moreover, list file 200 is written, when option 201B constituting list page 201 is specified, to produce a request message containing URL of explanatory file 207 ("http://www.ccc.co.jp/jkl.html") as a parameter of the GET method.

Also, SDF 204 contains "0001" as APID, information shown in Fig.7 as policy information, "http://www.main.bbb.co.jp/viewer.jam" as ADF-URL, and public key CA gives to IP which administers IP server unit 13 and IP server unit 14.

Also, in fixed memory 12A of IP server unit 12, are stored explanatory file 211 corresponding to Java-AP software of the title "tsume-shogi" (a game similar to "chess ") (hereinafter, referred to as the first Java-JP software), ADF 213, and Jar file 214. Explanatory file 211, ADF 213, and Jar file 214 are produced by IP administering IP server unit 12. The content of explanatory file 211 is shown in Fig.10. Explanatory file 211 is written to provide explanatory page 212 shown in Fig. 11 when interpreted and executed by mobile unit 16. Also, ADF 213 contains URL of Jar file 214 ("http://www.ccc.co.jp/shogi.jar") as package URL.

Also, in fixed memory 12A of IP server unit 12, are stored

explanatory file 207 corresponding to Java-AP software of the title "horoscope" (hereinafter, referred to as the second Java-AP software), ADF 209, and Jar file 210. Explanatory file 207, ADF 209, and Jar file 210 are produced by IP administering IP server unit 12. The content of explanatory file 207 is shown in Fig.12. Explanatory file 207 is written to provide explanatory page 208 shown in Fig. 13 when interpreted and executed by mobile unit 16. Also, ADF 209 contains URL of Jar file 210 ("http://www.ccc.co.jp/horoscope.jar") as package URL.

Also, in fixed memory 13A of IP server unit 13, are stored explanatory file 202 corresponding to Java-AP software of the title "telephone number directory viewer" (hereinafter, referred to as the third Java-AP software), ADF 205, and Jar file 206. Explanatory file 202, ADF 205, and Jar file 206 are produced by IP administering IP server unit 13 and IP server unit 14. The content of explanatory file 202 is shown in Fig.14. Explanatory file 202 is written to provide explanatory page 203 shown in Fig. 15 when interpreted and executed by mobile unit 16. ADF 205 contains "0001" as APID, the hash value of Jar file 206, URL of Jar file 206 ("http://www.main.bbb.co.jp/viewer.jar") as package URL, and is signed by secret key CA gives to IP administering IP server unit 13, and IP server unit 14.

Also, mobile unit 16 is in the status in which the first to the third Java-AP software can be downloaded.

(2-1) Installation Operation

First, the operation of installing Java-AP software in mobile unit 16 is explained with reference to each Java-AP software.

(2-1-1) First Java-AP Software

The installation operation of the first Java-AP software begins when the user finds the IP server unit in which Java-software he/she desires is stored, and then tries to obtain explanatory file 211 in the Web browser

by operating mobile unit 16. First, in mobile unit 16, request message tm 12 containing URL of explanatory file 211 ("http://www.ccc.co.jp/mno.html") as a parameter of the GET method is produced. Request message tm 12 is, as shown in Fig. 16, transmitted by mobile unit 16, and is received by IP server unit 12. In IP server unit 12, response message tm 13 containing explanatory file 211 is produced in response to the content of request message tm 12. Response message tm 13 is transmitted by IP server unit 12, and is received by mobile unit 16. In mobile unit 16, UI corresponding to the content of explanatory file 211 is provided to the user. As a result, in displaying unit 16C, explanatory page 212 shown, for instance, in Fig. 11 is displayed.

When the user sees explanatory page 212, and operates mobile unit 16 to hit anchor 212A in explanatory page 212, the value specified as ijam property of the anchor tag written in explanatory file 211 of Fig. 10 (the tag which begins with "<A") identifies the object tag specified as id property (the tag which begins with "<OBJECT") in mobile unit 16. Then, URL specified as data property of the object tag ("http://www.ccc.co.jp/shogi.jam") is extracted, and determination of Step S11 of Fig. 5 is carried out. In the present example, since the extension of URL is not sdf, the ordinary process (Step S12) is carried out. In other words, the process is carried out as follows. First, request message tm 16 for requesting transmission of ADF 213 identified by the URL is produced. Request message tm 16 is transmitted by mobile unit 16, and is received by IP server unit 12. In IP server unit 12, response message tm 17 containing ADF 213 is produced in response to the content of request message tm 16. Response message tm 17 is transmitted by IP server unit 12, and is received by mobile unit 16.

In mobile unit 16, on the basis of the content of ADF 213, whether the first Java-AP software can be installed is determined. As mentioned

above, since mobile unit 16 is in the status in which the first Java-AP software can be installed, installation of the first Java-AP software is determined to be possible in mobile unit 16.

Then, in mobile unit 16, ADF 213 is written into fixed memory 16D1. Also, in mobile unit 16, package URL ("http://www.ccc.co.jp/shogi.jar") is extracted from ADF 213, and request message tm 18 requesting transmission of Jar file 214 identified by the package URL is produced. Request message tm 18 is transmitted by mobile unit 16, and is received by IP server unit 12. In IP server unit 12, response message tm 19 containing Jar file 214 is produced in response to the content of request message tm 18. Response message tm 19 is transmitted by IP server unit 12, and is received by mobile unit 16. In mobile unit 16, Jar file 214 is written into fixed memory 16D1, and installation of the first Java-AP software is completed.

When the first Java-AP software is determined as not installable in mobile unit 16, the status of mobile unit 16 returns to the status that existed before the acquisition of ADF 213 began.

(2-1-2) Second Java-AP software

The installation operation of the second Java-AP software begins when the user tries to obtain explanatory file 207 by operating mobile unit 16. As already explained, explanatory file 207 can be obtained either by directly accessing the relevant IP server or through list file 200, but only the operation which begins with trying to obtain list file 200 is explained.

As shown in Fig. 17, in mobile unit 16, request message tm 20 containing URL of list file 200 ("http://www.aaa.co.jp/def.html") as a parameter of the GET method is produced. Request message tm 20 is transmitted by mobile unit 16, and is received by administering server unit 18. In administering server unit 18, response message tm 21 containing list file 200 is produced in response to the content of request message tm 20.

Response message tm 21 is transmitted by administering server unit 18, and is received by mobile unit 16. In mobile unit 16, when response message tm 21 is received, list file 200 in response message tm 21 is interpreted in accordance with HTML, and UI corresponding to the content of list file 200 is provided to the user of mobile unit 16. As a result, in displaying unit 16C of mobile unit 16, list page 201 shown, for instance, in Fig. 9 is displayed.

When the user, after seeing list page 201, operates mobile unit 16 to hit option 201B in list page 201, request message tm 22 containing URL ("http://www.ccc.co.jp.jkl.html") corresponding to option 201B as a parameter of the GET method is produced. Request message tm 22 is transmitted by mobile unit 16, and is received by IP server unit 12. In IP server unit 12, response message tm 23 containing explanatory file 207 is produced in response to the content of request message tm 22. Response message tm 23 is transmitted by IP server unit 12, and is received by mobile unit 16. In mobile unit 16, UI corresponding to the content of explanatory file 207 is provided to the user. As a result, in displaying unit 16C, explanatory page 208 shown, for instance, in Fig. 13 is displayed.

When the user, after seeing explanatory page 208, operates mobile unit 16 to hit anchor 208A in explanatory page 208, the value specified as ijam property of the anchor tag written in explanatory file 207 of Fig. 12 (the tag which begins with "<A") identifies the object tag specified as id property (the tag which begins with "<OBJECT"). Then, URL specified as data property of the object tag ("http://www.ccc.co.jp/horoscope.jam") is extracted, and determination of Step S11 of Fig.5 is carried out. In this example, since the extension of URL is not sdf, an ordinary process (Step S 12) is carried out. In other words, the process is carried out as follows. First, request message tm 26 requesting transmission of ADF 209 identified by the URL is produced. Request message tm 26 is transmitted by mobile

unit 16, and is received by IP server unit 12. In IP server unit 12, response message tm 27 containing ADF 209 corresponding to the content of request message tm 26 is produced. Response message tm 27 is transmitted by IP server unit 12, and is received by mobile unit 16.

In mobile unit 16, on the basis of the content of ADF 209, whether the second Java-AP software can be installed is determined. As mentioned above, since mobile unit 16 is in the status in which the second Java-AP software can be installed, the second Java-AP software is determined as installable in mobile unit 16.

Next, in mobile unit 16, ADF 209 is written into fixed memory 16D1. Also, in mobile unit 16, package URL ("http://www.ccc.co.jp/horoscope.jar") is extracted from ADF 209, and request message tm 28 requesting transmission of jar file 210 identified by package URL is produced. Request message tm 28 is transmitted by mobile unit 16, and is received by IP server unit 12. In IP server unit 12, response message tm 29 containing Jar file 210 in response to the content of request message tm 28 is produced. Response message tm 29 is transmitted by IP server unit 12, and is received by mobile unit 16. In mobile unit 16, Jar file 210 is written into fixed memory 16D1, and installation of the second Java-AP software is completed.

When the second Java-AP software is determined as not installable in mobile unit 16, the status of mobile unit 16 returns to a previous status, that which existed before the acquisition of ADF 209 began.

(2-1-3) Third Java-AP Software

The installation operation of the third Java-AP software begins when the user tries to obtain explanatory file 202 by operating mobile unit 16. In the operation, mobile unit 16 obtains relevant list file 200, determines where explanatory file 202 exists, and tries to obtain explanatory file 202.

As shown in Fig. 18, in the operation which begins by trying to obtain list file 200, an operation identical to the operation shown in Fig. 17 is carried out till list page 201 shown, for instance, in Fig. 9 is displayed after mobile unit 16 receives response message tm 21. When the user, after seeing list page 201, operates mobile unit 16 to hit option 201A in list page 201, request message tm 32 containing URL corresponding to option 201A ("http://www.main.bbb.co.jp/ghi.html") as a parameter of the GET method is produced in mobile unit 16. Request message tm 32 is transmitted by mobile unit 16, and is received by IP server unit 13. In IP server unit 13, response message tm 33 containing explanatory file 202 in response to the content of request message tm 32 is produced. Response message tm 33 is transmitted by IP server unit 13, and is received by mobile unit 16. In mobile unit 16, the user is provided with UI corresponding to the content of explanatory file 202. As a result, in displaying unit 16C, explanatory page 203 shown, for instance, in Fig. 15 is displayed.

When the user, after seeing explanatory page 203, operates mobile unit 16 to hit anchor 203A in explanatory page 203, the value specified as ijam property of the anchor tag written in explanatory file 202 in Fig. 14 (the tag which begins with "<A") identifies the object tag specified as id property (the tag which begins by "<OBJECT"). Then, URL specified as data property of the object tag ("http://www.aaa.co.jp/abc.sdf") is extracted, and determination of Step S11 in Fig. 5 is carried out. In the example, the extension of URL is sdf; therefore, the process of step S 13 and thereafter is carried out. In other words, the process is carried out as follows. First, request message tm 34 requesting transmission of SDF 204 identified by the URL is produced. Request message tm 34 is transmitted by mobile unit 16, and is received by administering server unit 18. In administering server unit 18, response message tm 35 containing SDF 204 in response to

the content of request message tm 34 is produced. Response message tm 35 is transmitted by administering server unit 18, and received by mobile unit 16 via gateway server unit 17 and mobile packet communication network 15. The communication path between administering server unit 18 and gateway server 17 is an exclusive line, and since gateway server unit 17 is directly connected to mobile packet communication network 15 whose security is assured, SDF 204 can not be falsified until SDF 204 is received by mobile unit 16 (thereinbefore, Step S13).

In mobile unit 16, SDF 204 is written into fixed memory 16D1 of fixed memory 16D. Also, in mobile unit 16, APID ("0001"), ADF-URL ("http://www.main.bbb.co.jp/viewer.jam"), and the public key are extracted from SDF 204, and request message tm 36 requesting transmission of ADF 205 identified by ADF-URL is produced. Request message tm 36 is transmitted by mobile unit 16, and is received by IP server unit 13. In IP server unit 13, response message tm 37 containing ADF 205 in response to the content of request message tm 36 is produced. Response message tm 37 is transmitted by IP server unit 13, and is received by mobile unit 16 (thereinbefore, Step S14).

In mobile unit 16, authenticity of ADF 205 is determined by using the public key extracted from SDF 204 (Step S15). As mentioned above, since the public key contained in SDF 204 corresponds to the key used for the signature on ADF 205, ADF 205 is determined to be authentic as far as ADF 205 is not changed in IP server unit 13, or on the communication path between IP server unit 13 and mobile unit 16.

When ADF 205 is determined to be authentic, in mobile unit 16, APID extracted from SDF 204 and APID contained in ADF 205 are compared (Step S16). As mentioned above, since APID which matches APID in SDF 204 is written in ADF 205 in IP server unit 13, APID extracted from SDF 204 and APID contained in ADF 205 match as long

as the description is correct.

When APID match, in mobile unit 16, whether the third Java-AP software can be installed is determined on the basis of the content of ADF 205 (Step S17). As mentioned above, since mobile unit 16 is in the status in which the third Java-AP software can be installed, the third Java-AP software is determined to be installable in mobile unit 16.

Then, in mobile unit 16, ADF 205 is written into fixed memory 16D1. Also, in mobile unit 16, the hash value and package URL ("http://www.main.bbb.co.jp/viewer.jar") are extracted, and request message tm 38 requesting transmission of Jar file 206 identified by the package URL is produced. Request message tm 38 is transmitted by mobile unit 16, and is received by IP server unit 13. In IP server unit 13, response message tm 39 containing Jar file 206 corresponding to the content of request message tm 38 is produced. Response message tm 39 is transmitted by IP server unit 13, and is received by mobile unit 16 (thereinbefore, Step S18).

In mobile unit 16, the hash value is calculated by using Jar file 206 and the specific hash function (Step S19), and the calculated hash value and the hash value extracted from ADF 205 are compared (Step S20). As mentioned above, the hash value of the Jar file corresponding to ADF 205 is written in ADF 205; therefore, these hash values would match as long as the description is correct. When these hash values match, in mobile unit 16, Jar file 206 is written into fixed memory 16D1, and the installation of the third Java-AP software is completed (Step S21 and S22).

When ADF 205 is determined to be not authentic in mobile unit 16, when APID extracted from SDF 204 and APID contained in ADF 205 do not match, when the third Java-AP software is determined to be not installable, or when the calculated hash value and the hash value extracted from ADF 205 do not match, a failure notice is sent to the user (Step S23),

and the status of mobile unit 16 returns to a previous status that which existed before the acquisition of SDF 204 began.

(2-2) Operation of Mobile Unit 16 When Java-AP Software Is Activated

Next, the operation of mobile unit 16 when Java-AP software is activated will be explained.

(2-2-1) Fist Java-AP Software

The operation of mobile unit 16, when the first Java-AP software installed by the above-mentioned installation operation is activated in mobile unit 16 in which JAM is achieved, and the functions corresponding to the software (hereinafter, referred to as the first Java-AP) are achieved will be explained.

When API, which the first Java-AP is about to use is non-trusted API, the use of the API is approved by JAM. Hence, the first Java-AP can use the API.

On the other hand, when API, which the first Java-AP is about to use is trusted API, JAM checks whether SDF corresponding to the Java-AP is stored in fixed memory 16D. Since such SDF is not stored in fixed memory 16D, JAM forbids the use of the API by the first Java-AP. Hence, the first Java-AP will not be able use the API.

(2-2-2) Second Java-AP Software

The operation of mobile unit 16 when the installed second Java-AP software is activated in mobile unit 16 in which JAM is achieved, and the functions corresponding to the software are achieved, is identical to the operation of mobile unit 16 when the first Java-AP software is activated.

(2-2-3) Third Java-AP Software

The operation of mobile unit 16 when the installed third Java-AP software is activated in mobile unit 16 in which JAM is achieved, and the functions corresponding to the software (hereinafter, referred to as the third

Java-AP) are achieved, will be explained.

When API, which the third Java-AP is about to use is non-trusted API, the use of the API is approved by JAM. Hence, the third Java-AP can use the API.

When API, which the third Java-AP is about to use is trusted API, the operation of mobile unit 16 depends upon the API. Hereinafter, the operation of mobile unit 16 is explained with regard to each API.

(2-2-3-1) getPhoneList()

Since "getPhoneList()" is trusted API, whether the API can be used is determined by JAM on the basis of policy information in SDF 204 stored in fixed memory 16D. The content of the policy information is the content shown in Fig. 7; therefore, the use of "getPhoneList()" is approved by JAM. Hence, the third Java-AP can use "getPhoneList()". In other words, the third Java-AP can read out telephone number directory data.

(2-2-3-2) getCallHistory()

Since "getCallHistory()" is trusted API, whether the API can be used is determined by JAM on the basis of policy information in SDF 204. Since the content of the policy information is the content shown in Fig. 7, the use of "getCallHistory()" is forbidden by JAM. Hence, the third Java-AP cannot use "getCallHitory()". In other words, the third Java-AP cannot read out history data of transmission and reception.

(2-3) Operation after Third Java-AP Software Is Changed

Next, the operation of the present system after IP, which administers IP server unit 13 and IP server unit 14 changes the transmission mode or the content of the third Java-AP software will be explained. However, the present change includes the change of the content of Jar file 206 for the purpose such as the improvement of the third Java-AP software, and the change of the transmission mode for the purpose such as alleviating the burden on IP server unit 13. To achieve the latter change, IP which

administers IP server unit 13 and IP server unit 14, as shown in Fig. 19, stores Jar file 206 after the change (hereinafter, referred to as Jar file 215) in fixed memory 14A of IP server unit 14, and produces ADF 216 by changing the content of ADF 205 in accordance with Jar file 215. The above-mentioned operation is required for transmission of the third Java-AP software after the change, and no operation is required for the communication provider, which administers administering server unit 18.

The installation operation of the third Java-AP software after such changes is shown in Fig. 20. The operation shown in Fig. 20 begins to differ from the operation shown in Fig. 18 when, in IP server unit 13, response message tm 47 containing ADF 216 is produced as opposed to response message tm 37 containing ADF 205. Response message tm 47 corresponds to response message tm 37, response message tm 48 corresponds to response message tm 38, and response message tm 49 corresponds to response message tm 39.

The operation after response message tm 47 is produced in IP server unit 13 essentially differs from the operation shown in Fig. 18 in that ADF 216 and Jar file 215 are the objects of the process; request message tm 48 requesting transmission of Jar file 215 identified by package URL contained in ADF 216 ("http://www.sub.bbb.co.jp/viewer.jar") is produced in mobile unit 16; request message tm 48 is transmitted by mobile unit 16, and received by IP server unit 14; response message tm 49 containing Jar file 215 is produced in IP server unit 14; and response message tm 49 is transmitted by IP server unit 14, and is received by mobile unit 16.

(3) Modification

In the above-mentioned transmission system, ADF and a Jar file are transmitted by the IP server unit, but one or both of these can be transmitted by the administering server unit.

Also, in the above-mentioned transmission system, the mobile unit

confirms the authenticity of the correspondence of the producer of SDF with the producer of ADF on the basis of signature data using the secret key and the public key, but the length of the process in the mobile unit and the IP server unit, or the amount of communication among the mobile unit, the administering server unit, and the IP server unit can be alleviated by not including the public key in SDF; by not signing ADF by using the secret key in the IP server unit; or by omitting the confirmation process in the mobile unit, according to the security level required for the system.

Also, in the above-mentioned transmission system, the hash value of the Jar file is included in ADF corresponding to the Jar file; and the hash value is calculated in the mobile unit; then the authenticity of the correspondence of the Jar file and ADF is confirmed by comparing the hash value in ADF to the calculated hash value, but the length of the process in the mobile unit and the IP server unit and the amount of communication between the mobile unit and the IP server unit can be alleviated by omitting the confirmation process without including the hash value in ADF depending upon the security level required for the system.

Also, in the above-mentioned transmission system, whether the correspondence of SDF with ADF (and the Jar file) is authentic is determined by using the inherent APID to trusted Java-AP, but authenticity of the correspondence of SDF with ADF (and the Jar file) can be determined by using the CID inherent to the information provider, which provides trusted Java-AP. Also, depending upon the security level required for the system, the determination made on the basis of APID and CID can be omitted.

Also, in the above-mentioned transmission system, the server is specified by using the domain name, but the server can also be specified by using the IP address.

Also, in the mobile unit, by comparing the domain name of the

server unit, which transmits SDF to a preset letter string, SDF can be determined to be authentic only when the domain name is that of a server unit administered by a trustworthy organization. In this mode, the letter string to be compared (for instance, the letter string showing the domain name of the communication provider) is pre-stored in ROM or the fixed memory of the mobile unit. When the letter string is pre-stored in ROM, higher security can be assured since the letter string cannot be rewritten. Also, if the letter string is pre-stored in the fixed memory, trustworthy organizations can be stored after the purchase of the mobile unit; therefore, excellent convenience can be provided to a user and a trustworthy organization.

Also, in the above-mentioned transmission system, a high level of security is assured with a communication provider, which provides the communication path used for transmission of SDF as a trustworthy organization, but the technological scope of the present invention includes the mode in which the communication path is not provided by a trustworthy organization. For instance, by connecting a trustworthy organization to a mobile unit by using an encrypted communication path, the trustworthy organization can transmit SDF via the encrypted communication path. Also, even if the security of the communication path is not assured, by transmitting after encrypting SDF, and decoding SDF in the mobile unit, SDF can be transmitted with a certain degree of security.

In the above-mentioned transmission system, a file is transmitted and received in accordance with HTTP, but the system can be modified to assure higher security by using HTTPS.

Also, in the above-mentioned transmission system, a trustworthy organization can be an IP, in other words, the administering unit could comprise an IP server unit.

Moreover, in the above-mentioned transmission system, API is the object for restricting the use by Java-AP, but any resource can be the object. The resource can be a hardware resource. Also, the resource can be a network resource, or a software resource. A hardware resource can be a resource such as a memory, a speaker, a microphone, an infrared controller, LED (Light Emitting Diode) which a mobile unit can be equipped with, or an external hardware box such as UIM (User Identity Module) or SIM (Subscriber Identity Module) which functions with the mobile unit.

Next, a network resource is explained. As mentioned above, the mobile unit performs radio communication with the mobile communication network. During radio communication, the mobile unit uses a radio resource such as a radio channel provided by the mobile communication network. The radio resource is one of network resources. Also, the mobile unit, in a higher communication protocol layer than the communication protocol layer the radio resource belongs to, uses a communication resource such as a transmission path of packets or a communication path of the connecting network. The communication resources such as these are included as a network resource.

Next, a software resource is explained. A software resource can be API, a class, a package and so forth. Various functions are provided by a software resource, but a typical function can be a computation process such as encryption computation, or a function of transmitting or receiving data with other applications such as a Web browser. Also, the technological scope of the present invention includes the mode of restricting the use of a software resource, which the above-mentioned external hardware box is equipped with.

Incidentally, the use of a hardware resource or a network resource by Java-AP generally takes place by using a software resource. A mobile unit of the above-mentioned transmission system is also equipped with a

software resource to use a hardware resource or a network resource, and by restricting the use of a software resource of this type; the use of a hardware resource or a network resource is indirectly restricted. By indirectly restricting in this manner, and by preparing various software resources, restrictions which cannot be achieved unless restriction on a plurality of resources are changed in detail, such as giving the right to change the authorization of Java-AP to only trusted Java-AP, lifting the restriction on allowing to communicate only with a server unit accessed for downloading, or allowing to access a specific memory domain can easily be specified. Also, the mode of indirectly restricting the use of a software resource of the above-mentioned external hardware box by restricting the use of a software resource installed in the mobile unit is included in the technological scope of the present invention.

With regard to a method of expressing permission, a flag (permit/forbid) corresponding to one resource can be used, or permissions of a plurality of resources can be denoted by one expression.

Also, in the present invention, permission can be denoted to permit (or forbid) the use of a resource with a plurality of types. In this case, in the mobile unit, a more precise control can be achieved. For instance, since two modes (reading out and writing in) exist in the memory, the memory can be used for both reading out and writing in by trusted Java-AP although memory is used only for reading out by non-trusted Java-AP. Also, for instance, when the Web browser and so forth are activated while Java-AP with the right to use a packet transmission path is activated in a mobile unit in which a plurality of applications can share one packet transmission path, control can be such that Java-AP which is permitted to "exclusively use a packet transmission path" can exclusively use a packet transmission path although the Java-AP which is not permitted to "exclusively use a packet transmission path" cannot exclude the sharing of

packet transmission path by a Web browser and so forth. Also, by further modifying the above-mentioned modification, the following control can be possible. In other words, Java-AP with a certain type of permission can exclusively use the packet communication path without the user's consent. Also, Java-AP with another permission can use the packet communication path without the user's consent, but needs to obtain the user's consent to exclusively use the packet communication path. Also, Java-AP with another permission can use the packet communication path without the user's consent, but cannot exclusively use the packet communication path. Also, Java-AP with another permission can use the packet communication path only with the user's permission. Also, Java-AP with another permission cannot even use the packet communication path. As it is obvious from these examples, "types of use" of the present invention also contain types of a process when a resource is used (a process of obtaining the user's consent/ a process of not obtaining the user's consent)

Also, in the above-mentioned transmission system, an identical list page is provided for all mobile units, but a different list page can be provided for each mobile unit.

Also, in the above-mentioned transmission system, the operation of Java-AP is restricted when the Java-AP is executed. Instead, by including policy information in the Jar file stored in the IP server unit, and when the Jar file is downloaded in the mobile unit, activation of the Java-AP corresponding to the Jar file, or installation of Java-AP software containing the Jar file can be forbidden if comparison between the policy information and the policy information in SDF results in a mismatch. Only the permission given to the item as a result of the match in policy information can be valid.

Also, SDF can be transmitted after being signed by the secret key,

2003201905 05 Feb 2007

which CA gives to the communication provider, and the signature on SDF can be inspected in the mobile unit by the public key, which CA gives to the communication provider. The public key of the communication provider must necessarily be pre-stored in the mobile unit. The public key can be pre-stored in the fixed memory after being transmitted by means of communication. Also, the mobile unit can be sold after writing the key into ROM.

Also, in the above-mentioned transmission system, software is delivered to a mobile unit, but the technological scope of the present invention includes the mode of transmitting software to a terminal unit besides a mobile unit.

Comprises/comprising and grammatical variations thereof when used in this specification are to be taken to specify the presence of stated features, integers, steps or components or groups thereof, but do not preclude the presence or addition of one or more other features, integers, steps, components or groups thereof.

2003201905 05 Feb 2007

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A transmission method including:

a process for transmitting an authorization file in a communication system in which an originator originates a request including information showing a storage of a file and the file is transmitted in response to said request, said process for transmitting including transmitting a security descriptive file as said authorization file from an administering server unit storing said security descriptive file through a secure link to a terminal unit, the security descriptive file containing first identification information and authorization information, the first identification information showing a storage location of an application descriptive file, the application descriptive file having information dependent upon an entity file, which includes software for executing an application, along with information showing a storage location of said entity file, the authorization information of the security descriptive file indicating an allowable range of an operation of the application which is executed in accordance with said software, said terminal unit executing operation of the application within a range shown by said authorization information;

a dependent information obtaining process for said terminal unit to obtain, by using said first identification information contained in said security descriptive file transmitted from said communication system in said authorization transmission process, said application descriptive file from one or a plurality of server units in which said application descriptive file is stored; and

a program obtaining process for said terminal unit to obtain said entity file from said communication system by using said application descriptive file obtained in said dependent information obtaining process.

2. The transmission method according to Claim 1,

wherein said application descriptive file is obtained from said administering server unit by said dependent information obtaining process.

3. The transmission method according to Claim 1,

2003201905 05 Feb 2007

wherein said entity file is obtained from said administering server unit by said program obtaining process.

4. The transmission system according to Claim 1,

wherein said application descriptive file is obtained from said administering server unit in said dependent information obtaining process, and

wherein said entity file is obtained from said administering server unit in said program obtaining process.

5. The transmission method according to Claim 1 further including:

an encryption process for said communication system to encrypt said security descriptive file; and

a decoding process for said terminal unit to decode said security descriptive file transmitted by said communication system in said process for transmitting an authorization file,

wherein, in said process for transmitting an authorization file, said security descriptive file encrypted in said encryption process is transmitted to said terminal unit, and

wherein, in said dependent information obtaining process, said terminal unit obtains said application descriptive file by using said security descriptive file decoded in said decoding process.

6. The transmission process according to Claim 1,

wherein said authorization information shows restriction on use of a resource.

7. The transmission method according to Claim 6,

wherein said resource is a hardware resource inside said terminal unit.

8. The transmission method according to Claim 6,

wherein said resource is a hardware resource outside said terminal unit which said terminal unit can use.

2003201905 05 Feb 2007

9. The transmission method according to Claim 6,
wherein said resource is a software resource inside said terminal unit.

10. The transmission method according to Claim 6,
wherein, said resource is a software resource outside said terminal unit which said terminal unit can use.

11. The transmission method according to Claim 6,
wherein said resource is a network resource which said terminal unit can use.

12. The transmission method according to Claim 1,
wherein said authorization information shows a type of use of a resource.

13. The transmission method according to Claim 1,
wherein an application descriptive file corresponding to said application is signed by a secret key a certifying agent gives to an information provider providing said application,
wherein a security descriptive file corresponding to said application contains a public key a certifying agent gives to said information provider, and
wherein, in said program obtaining process, said terminal unit inspects authenticity of an application descriptive file obtained in said dependent information obtaining process by using said public key, and obtains said entity file from said communication system by using said application descriptive file only when authenticity is verified.

14. The transmission method according to Claim 1,
wherein said application descriptive file and said security descriptive file contain an application identifier an administrator which administers said administering server unit gives, and
wherein, in said program obtaining process, said terminal unit compares an application identifier contained in a security descriptive file transmitted by said administering server unit in said authorization transmission process to an application identifier contained in an application descriptive file obtained in said

2003201905 05 Feb 2007

dependent information obtaining process, and obtains said entity file from said communication system by using said application descriptive file only when both identifiers match.

15. The transmission method according to Claim 1,

wherein said communication system further includes an information providing server unit in which a file for downloading containing a second identification information showing a stored location of said security descriptive file;

an advance transmission process for said communication system to transmit said file for downloading to a terminal unit; and

a process for requesting transmission of an authorization file for said terminal unit to request said communication system for transmission of said security descriptive file by using said file for downloading transmitted by said communication system in said advance transmission process,

wherein, in said authorization transmission process, said communication system transmits to said terminal unit said security descriptive file requested by said process for requesting transmission of an authorization file.

16. The transmission method according to Claim 1,

wherein a process after said dependent information obtaining process is carried out only when a security descriptive file transmitted in said dependent information transmission process is stored in said administering server unit.

17. The transmission method according to any one of Claim 1 to Claim 16, wherein said terminal unit is a mobile unit.

18. A transmission system including:

a communication system for returning, when a stored location of a file is notified, said file which includes one or a plurality of server units in which an entity file containing software for achieving an application and an application descriptive file which has a content dependent upon said entity file showing a stored location of said entity file, and an administering server unit in which a security descriptive file containing a first identification information showing a stored location of said application descriptive file and authorization information showing authorization

2003201905 05 Feb 2007

given to an application which is achieved when a terminal unit executes said software is stored; and

a terminal unit which approves operation of an application in accordance with authorization given to said application,

wherein said administering server unit transmits said security descriptive file to said terminal unit by assuring security, and

wherein said terminal unit obtains said application descriptive file by using said first identification information contained in said security descriptive file transmitted by said communication system, and said entity file from said communication system by using said application descriptive file.

19. The transmission system according to Claim 18,

wherein said administering server unit stores said application descriptive file.

20. The transmission system according to Claim 18,

wherein said administering server unit stores said entity file.

21. The transmission system according to Claim 18,

wherein, said administering server unit stores said application descriptive file, and

wherein said administering server unit stores said entity file.

NTT DOCOMO, INC.

WATERMARK PATENT & TRADE MARK ATTORNEYS

P24327AU00

FIG. 1

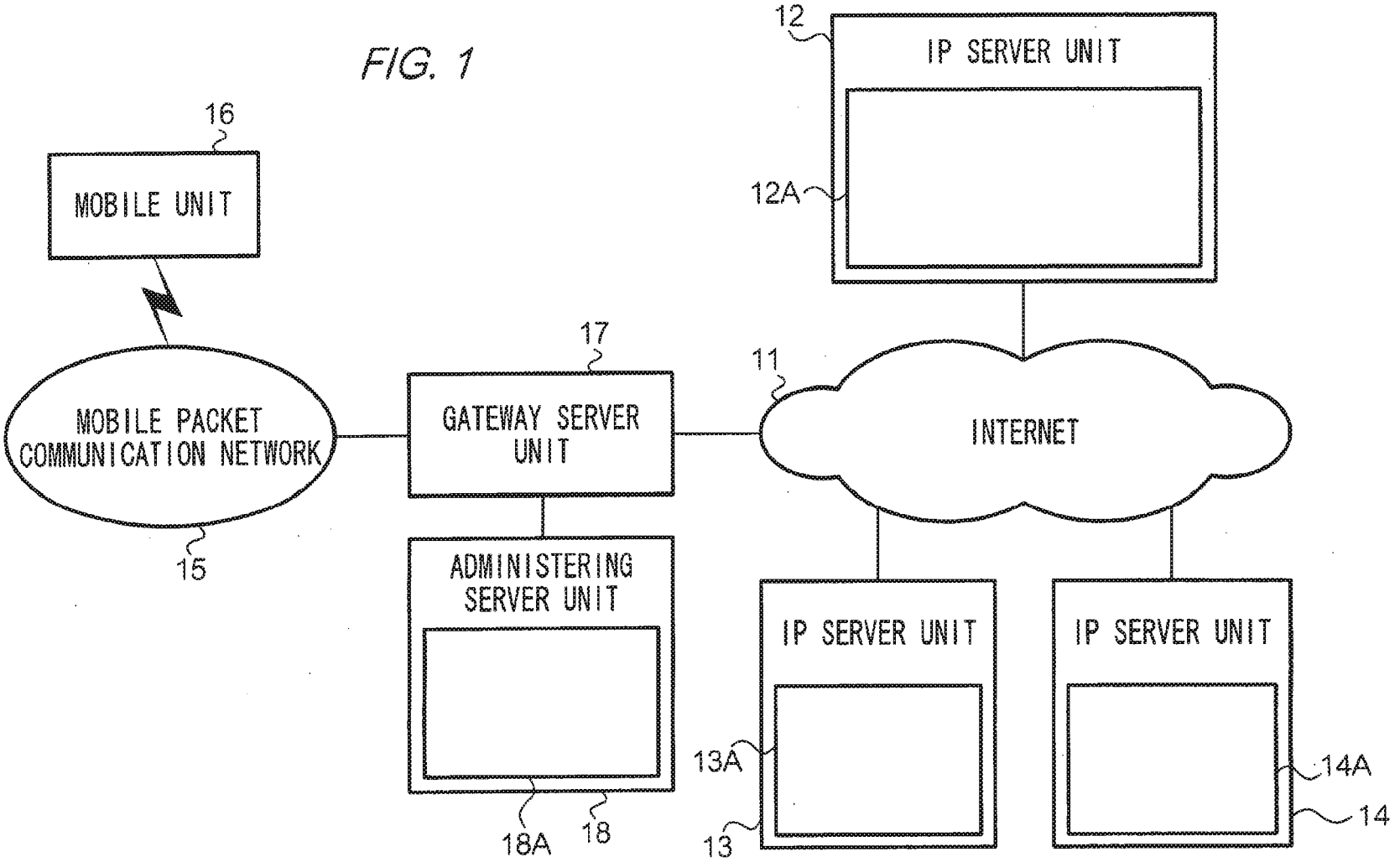

12
IP SERVER UNIT
12A
16
MOBILE UNIT
17
11
MOBILE PACKET COMMUNICATION NETWORK
GATEWAY SERVER UNIT
INTERNET
15
ADMINISTERING SERVER UNIT
IP SERVER UNIT
IP SERVER UNIT
13A
14A
18A
18
13
14

FIG. 2

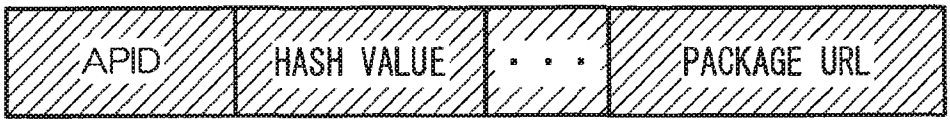
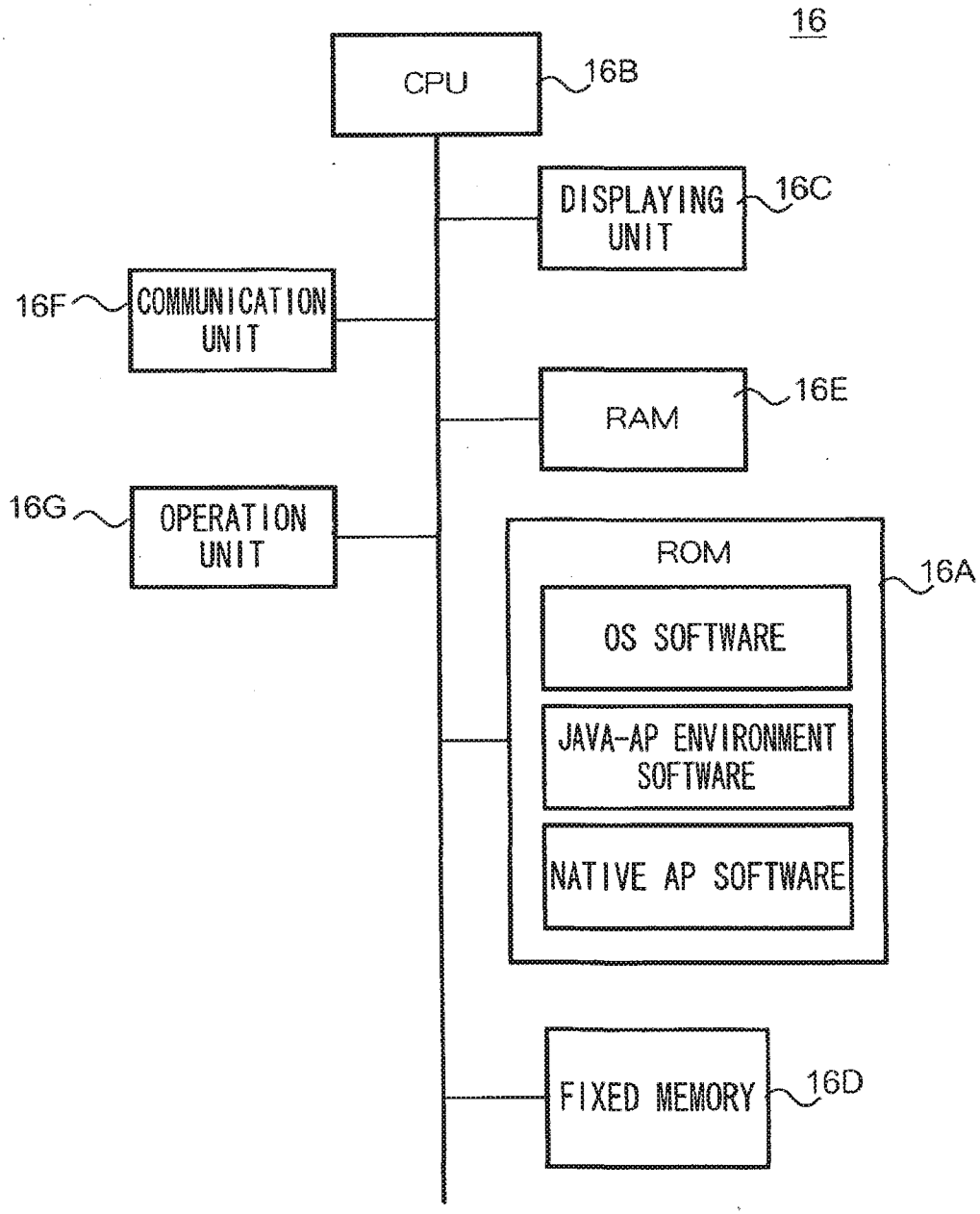

APID
HASH VALUE
• • •
PACKAGE URL

FIG. 3


16
CPU
16B
DISPLAYING UNIT
16C
16F
COMMUNICATION UNIT
RAM
16E
16G
OPERATION UNIT
ROM
16A
OS SOFTWARE
JAVA-AP ENVIRONMENT SOFTWARE
NATIVE AP SOFTWARE
FIXED MEMORY
16D

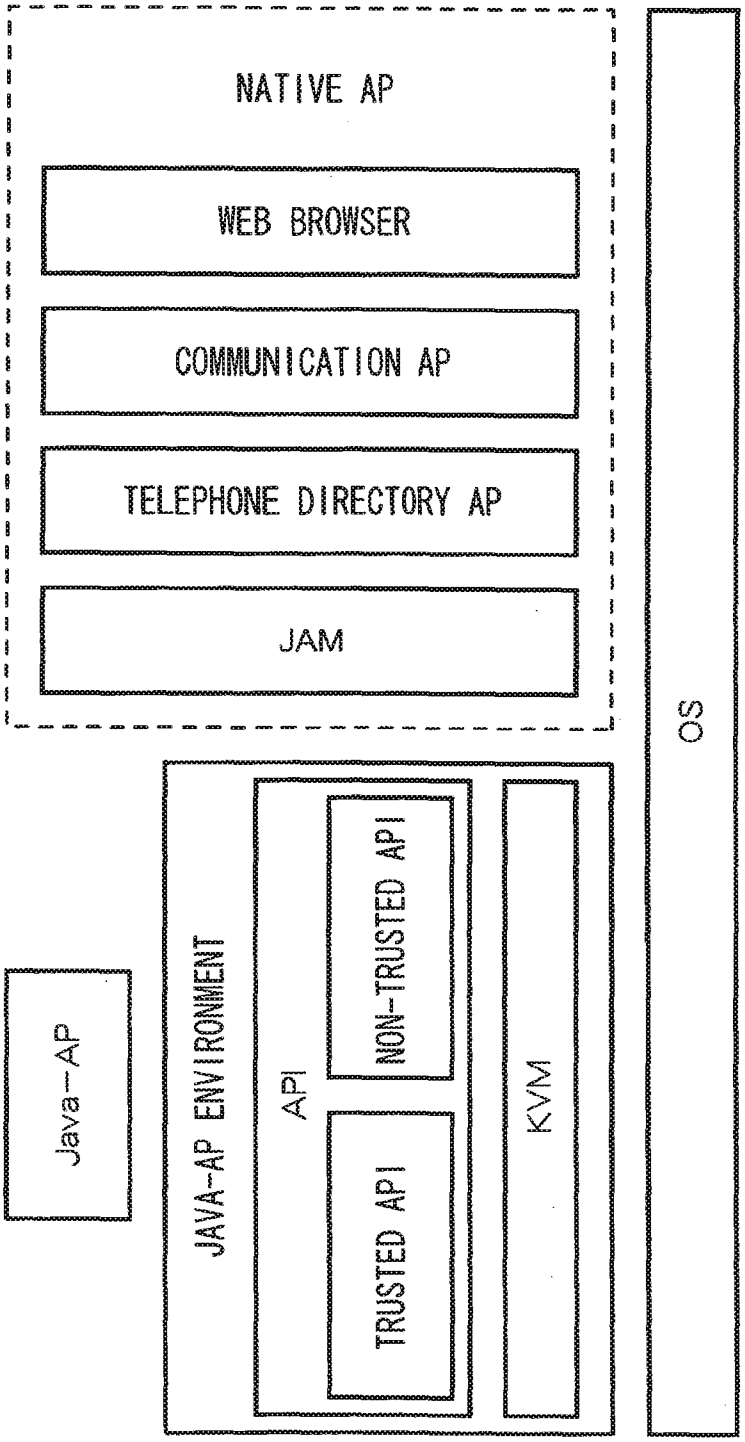

NATIVE AP
WEB BROWSER
COMMUNICATION AP
TELEPHONE DIRECTORY AP
JAM
OS
JAVA-AP ENVIRONMENT
API
NON-TRUSTED API
TRUSTED API
KVM
Java-AP

FIG. 4

FIG. 5

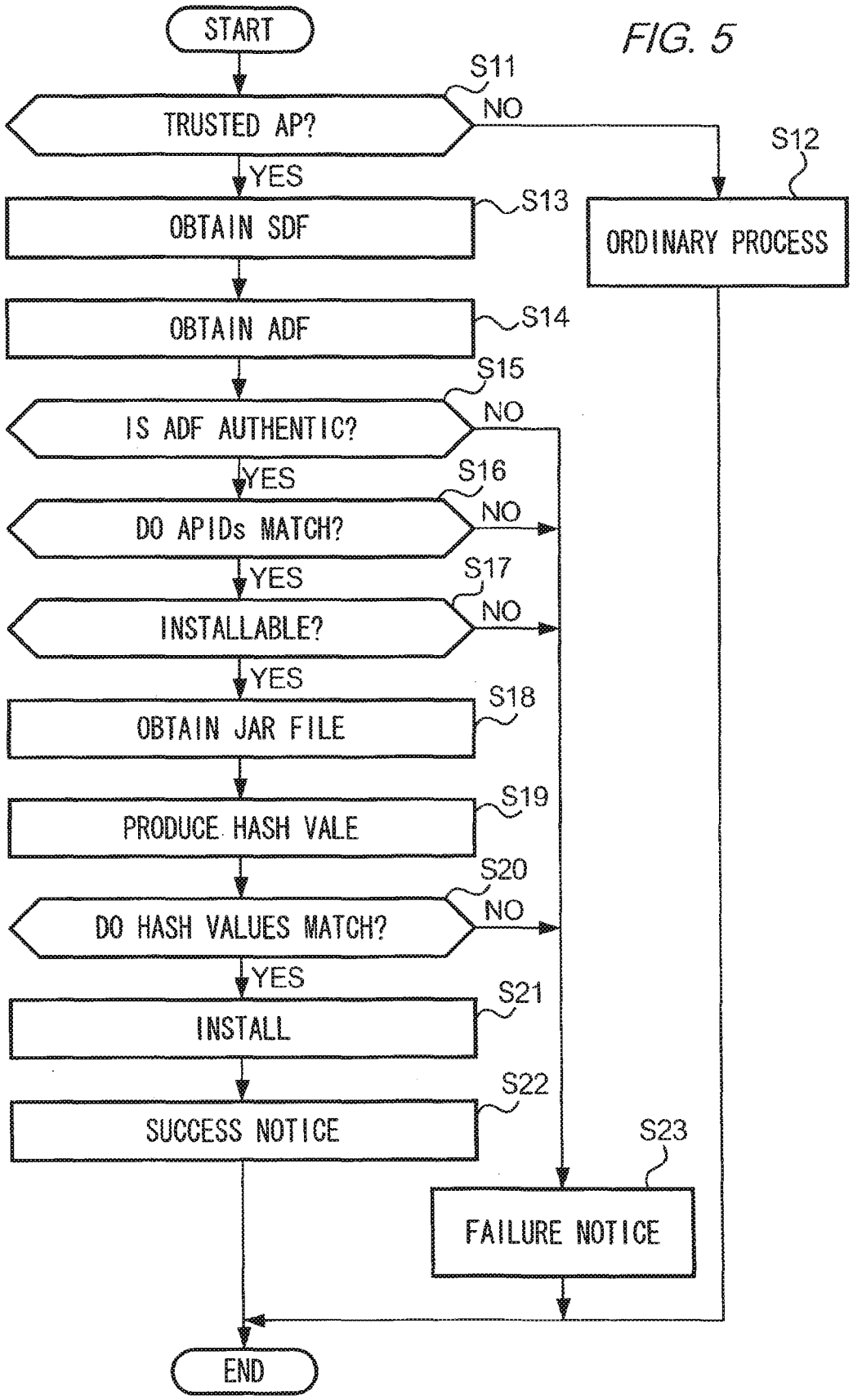

START
S11
TRUSTED AP?
NO
S12
YES
S13
OBTAIN SDF
ORDINARY PROCESS
S14
OBTAIN ADF
S15
IS ADF AUTHENTIC?
NO
YES
S16
DO APIDs MATCH?
NO
YES
S17
INSTALLABLE?
NO
YES
S18
OBTAIN JAR FILE
S19
PRODUCE HASH VALE
S20
DO HASH VALUES MATCH?
NO
YES
S21
INSTALL
S22
SUCCESS NOTICE
S23
FAILURE NOTICE
END

FIG. 6

APID	POLICY INFORMATION	ADF-URL	PUBLIC KEY

FIG. 7

TRUSTED API	PERMISSION
getPhoneList()	○
getCallHistory()	×
getMsStatus()	○

FIG. 8

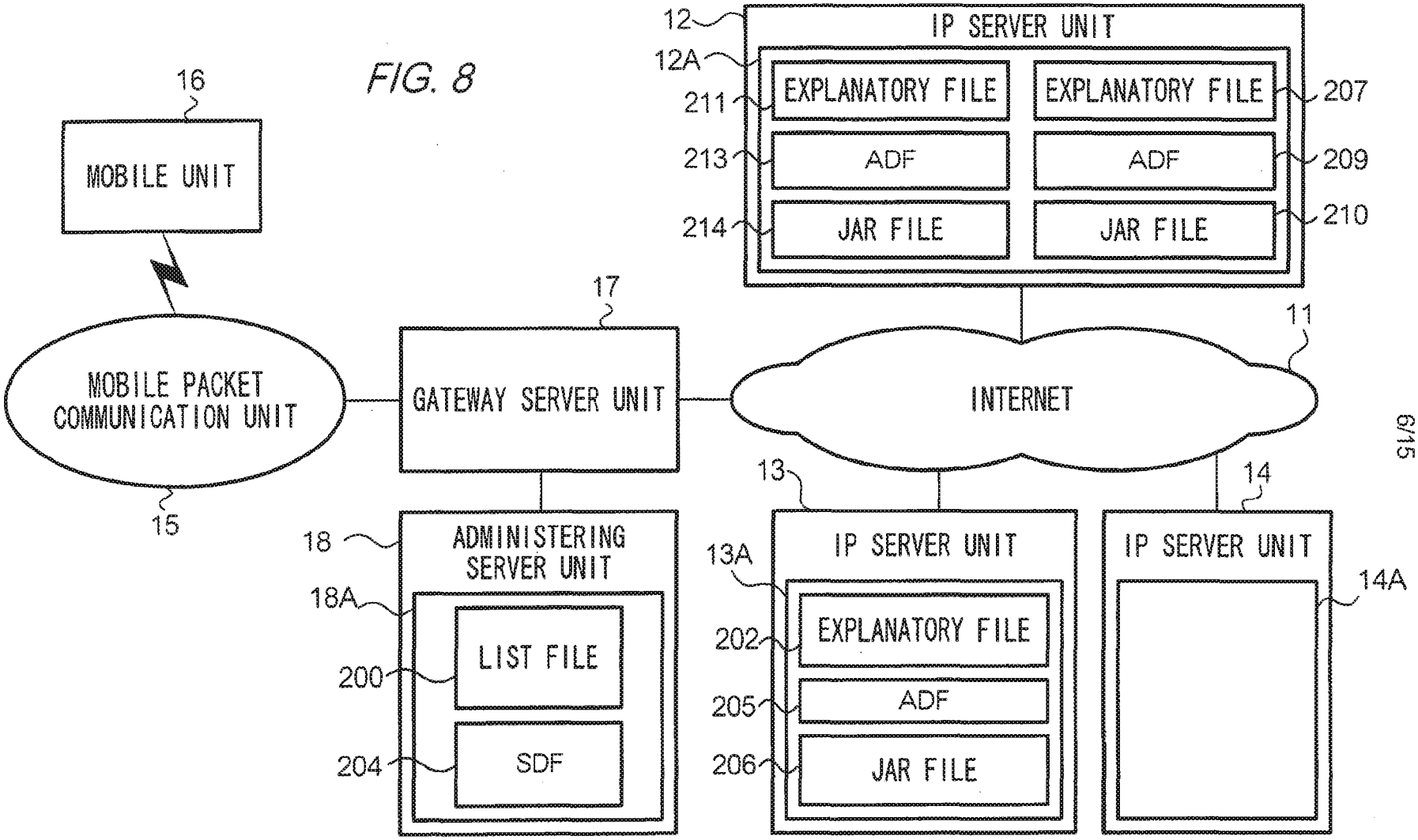

12
IP SERVER UNIT
12A
EXPLANATORY FILE
EXPLANATORY FILE
207
211
213
ADF
ADF
209
214
JAR FILE
JAR FILE
210
16
MOBILE UNIT
17
11
MOBILE PACKET COMMUNICATION UNIT
GATEWAY SERVER UNIT
INTERNET
15
13
14
18
ADMINISTERING SERVER UNIT
IP SERVER UNIT
IP SERVER UNIT
13A
14A
18A
LIST FILE
EXPLANATORY FILE
202
200
ADF
205
204
SDF
JAR FILE
206

FIG. 9

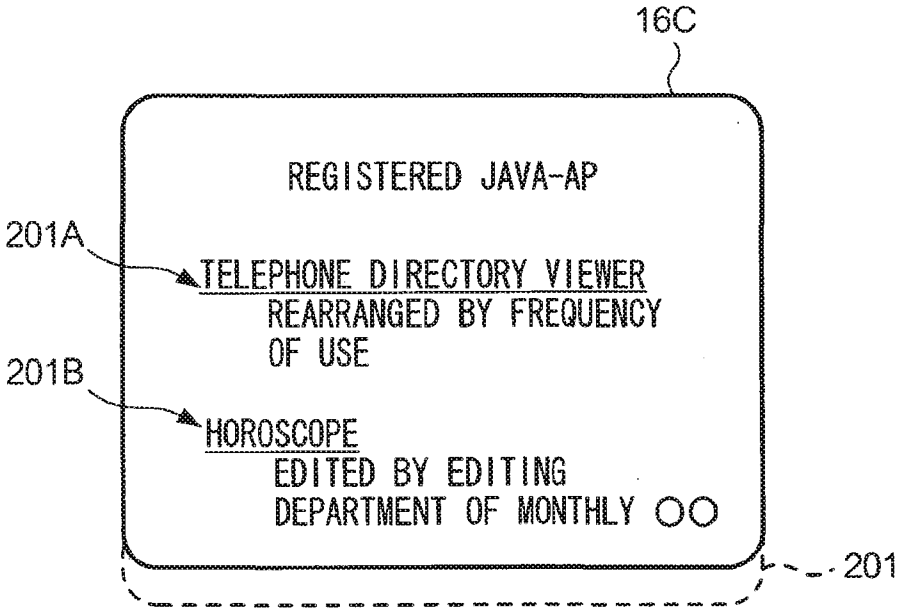


FIG. 10

<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/horoscope.jam>
TSUME-SHOGI
</OBJECT>
SOFTWARE FOR ～.CLICK
<A ijam="#application.declaration">HERE</A>
TO DOWNLOAD.

FIG. 11

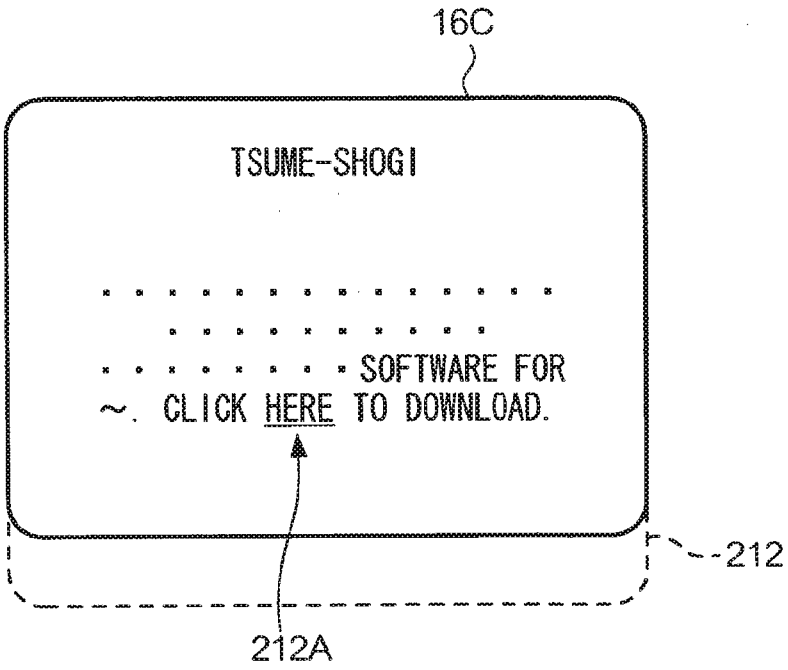


FIG. 12

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/viewer.jam>
HOROSCOPE
</OBJECT>
SOFTWARE FOR ~. CLICK
<A ijam="#application.declaration">HERE</A>
TO DOWNLOAD.
```

FIG. 13

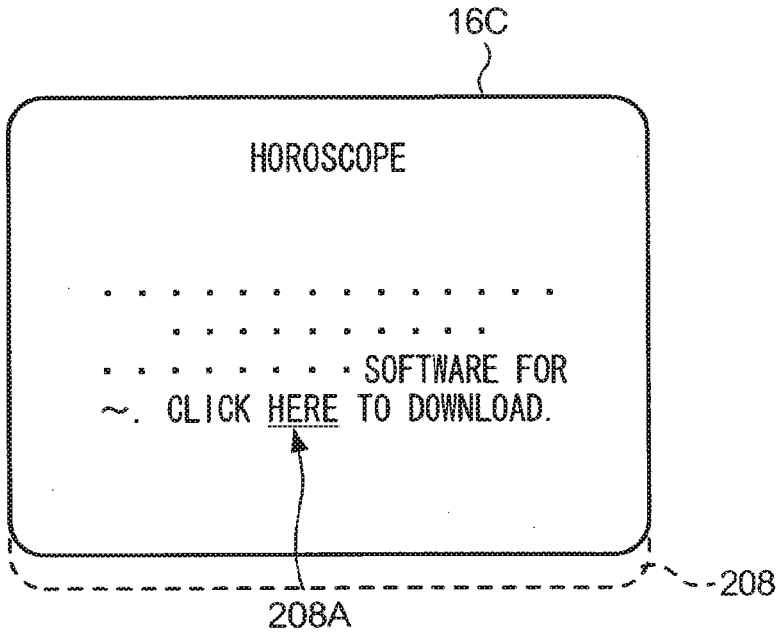


FIG. 14

```
<OBJECT declare id="application.declaration"
data="http://www.aaa.co.jp/abc.sdf"
type="application/x-jam">
TELEPHONE DIRECTORY VIEWER
</OBJECT>
SOFTWARE FOR ~. CLICK
<A ijam="#application.declaration">HERE</A>
TO DOWNLOAD.
```

FIG. 15

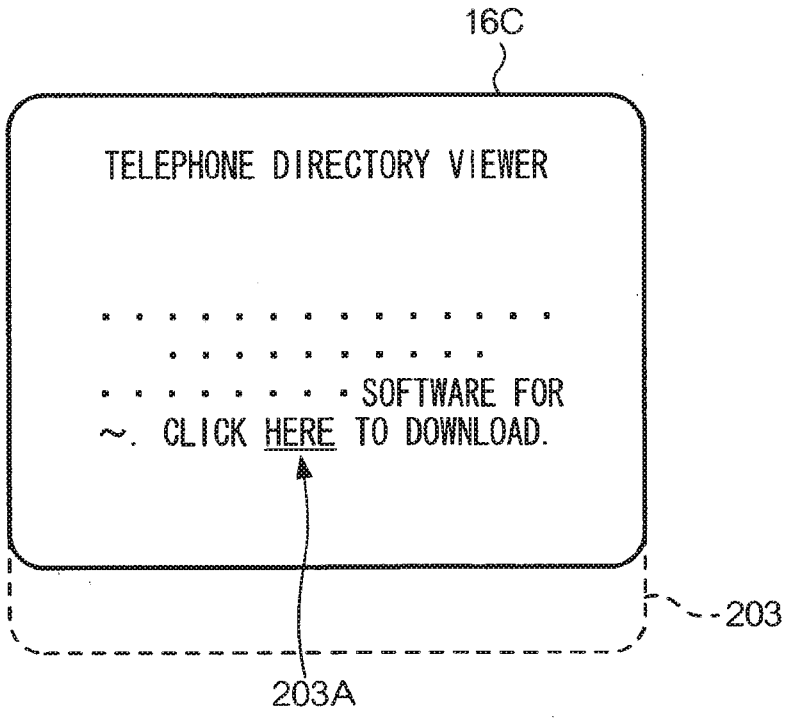

16C
TELEPHONE DIRECTORY VIEWER
SOFTWARE FOR
~. CLICK HERE TO DOWNLOAD.
203
203A

FIG. 16

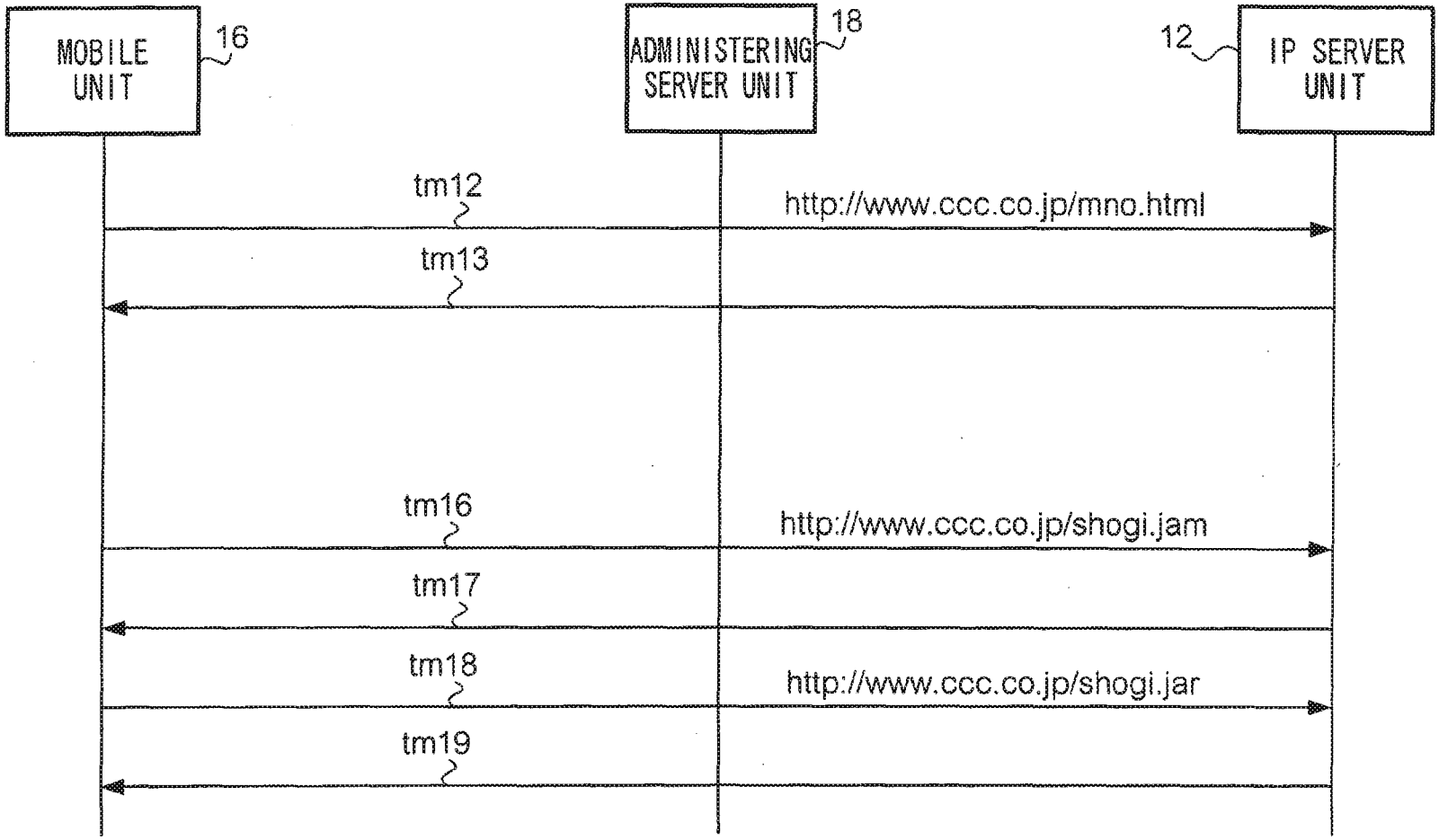

MOBILE UNIT
16
ADMINISTERING SERVER UNIT
18
12
IP SERVER UNIT
tm12
http://www.ccc.co.jp/mno.html
tm13
tm16
http://www.ccc.co.jp/shogi.jam
tm17
tm18
http://www.ccc.co.jp/shogi.jar
tm19

FIG. 17

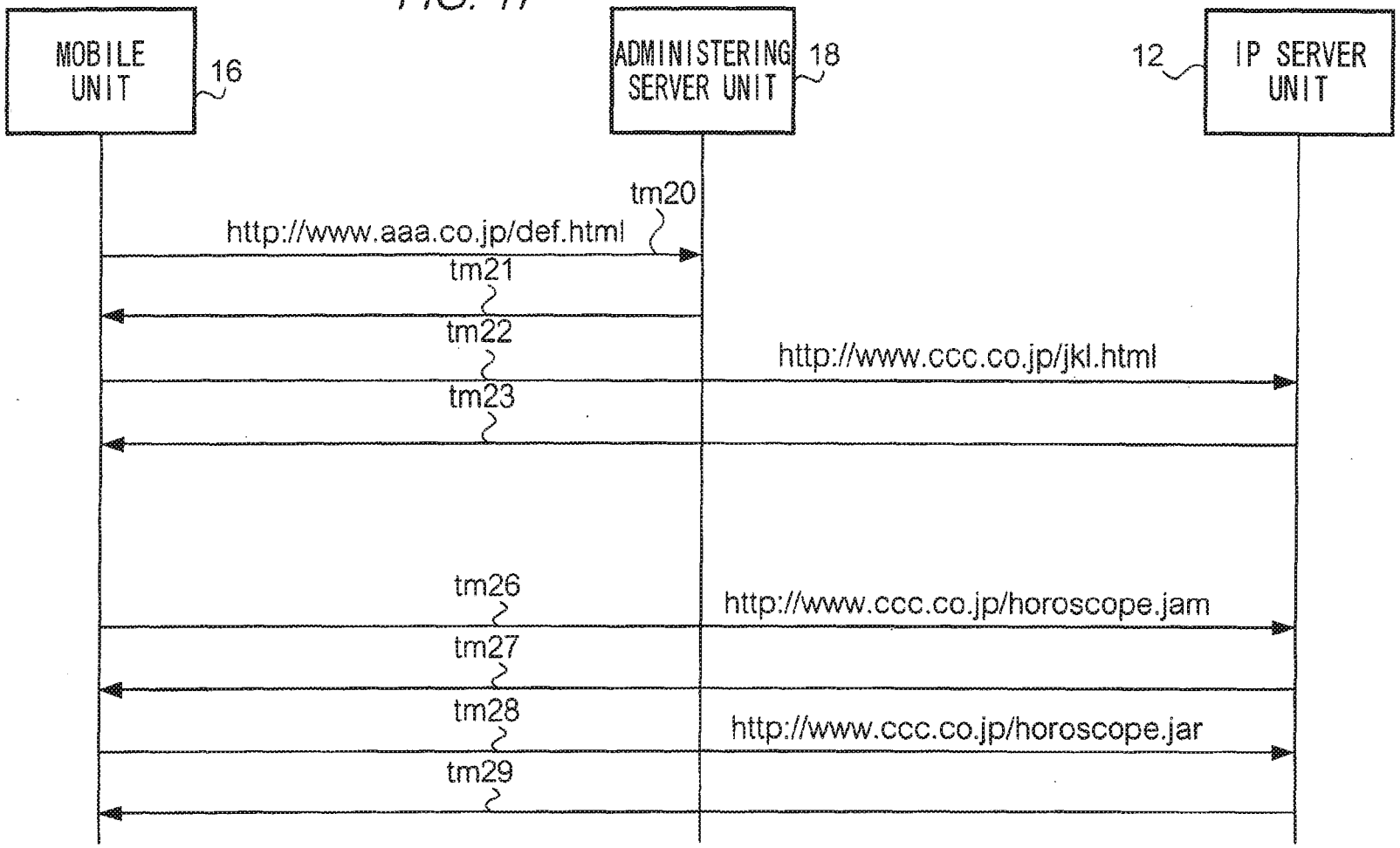

MOBILE UNIT
16
ADMINISTERING SERVER UNIT
18
12
IP SERVER UNIT
tm20
http://www.aaa.co.jp/def.html
tm21
tm22
http://www.ccc.co.jp/jkl.html
tm23
tm26
http://www.ccc.co.jp/horoscope.jam
tm27
tm28
http://www.ccc.co.jp/horoscope.jar
tm29

FIG. 18

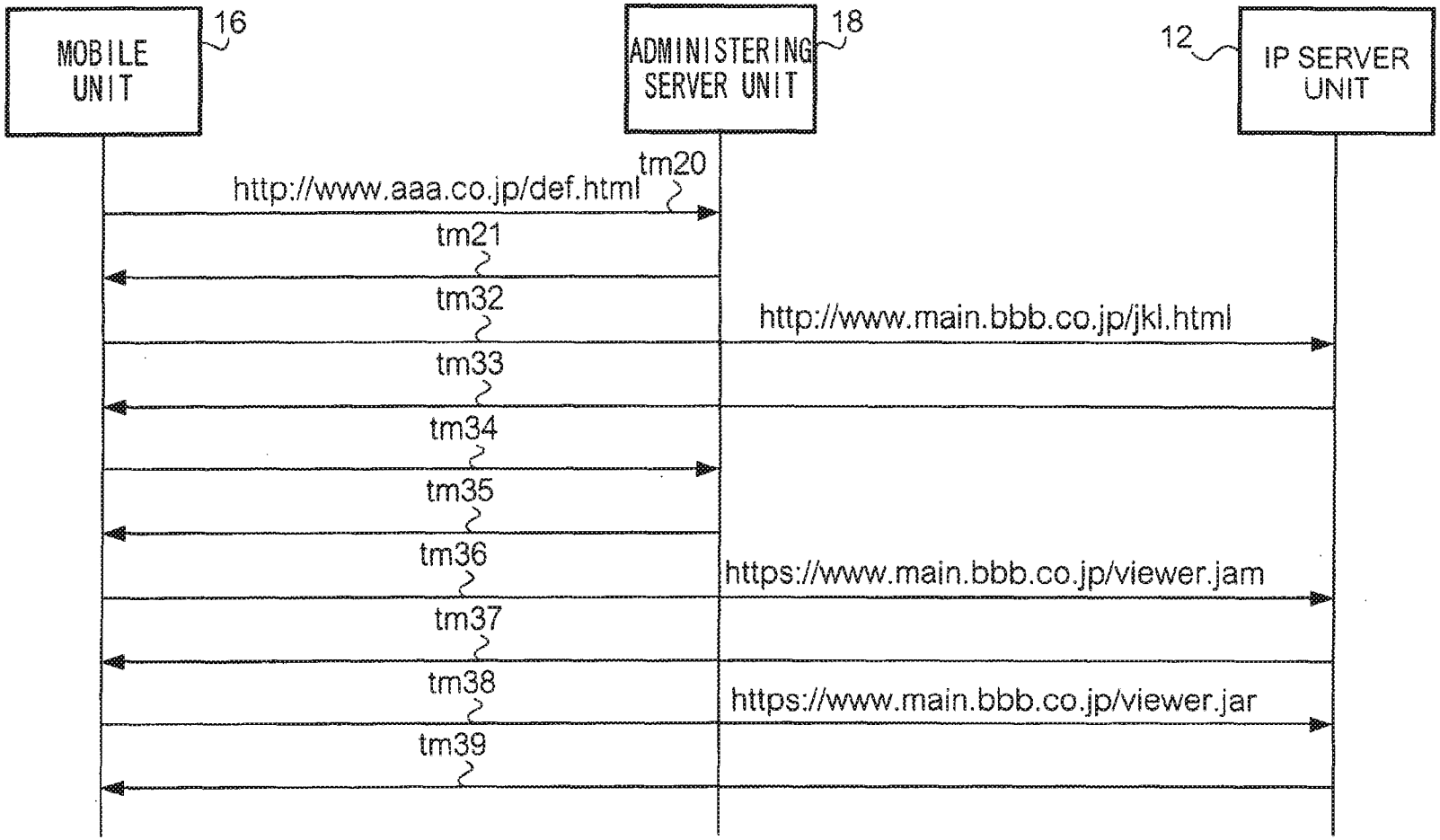
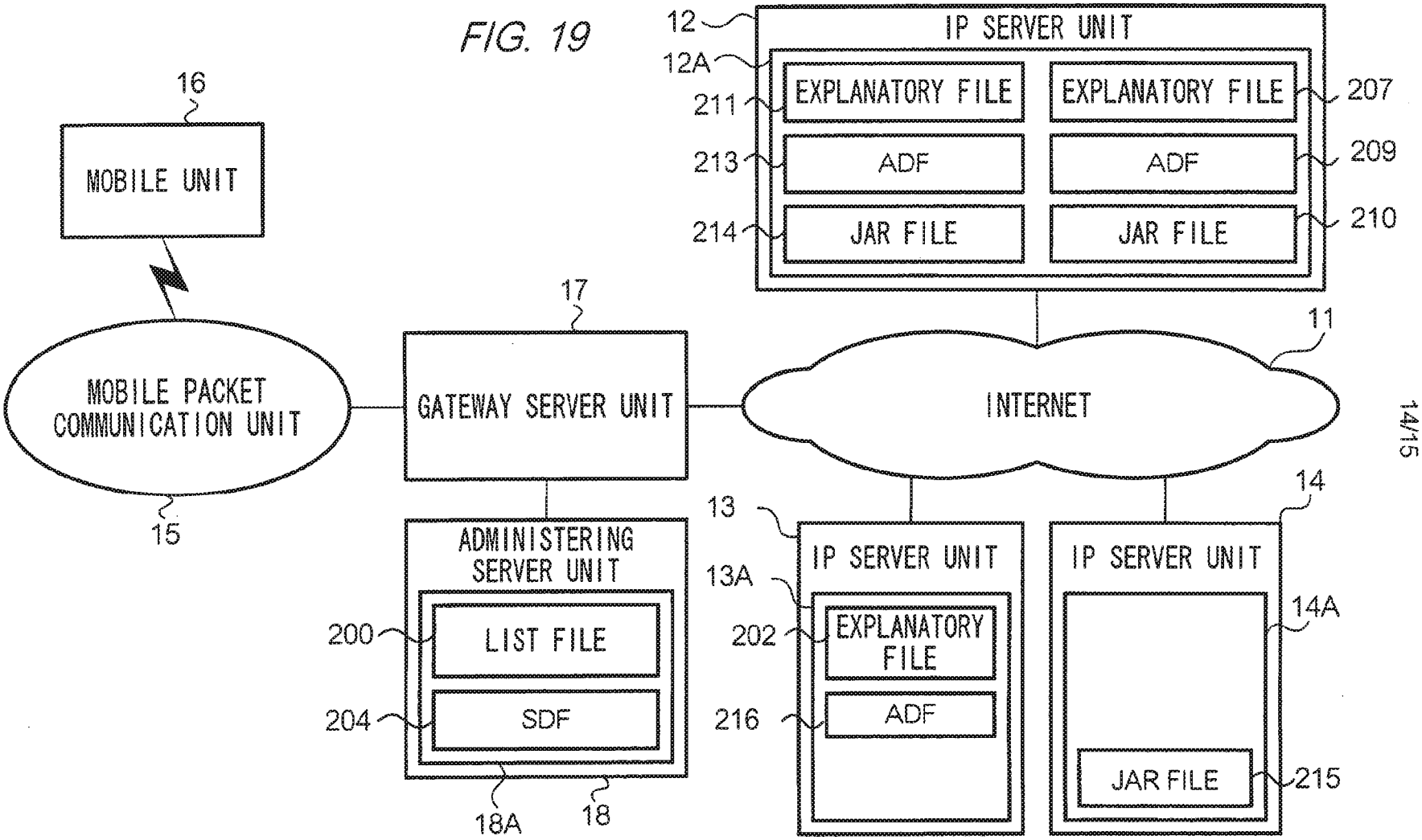
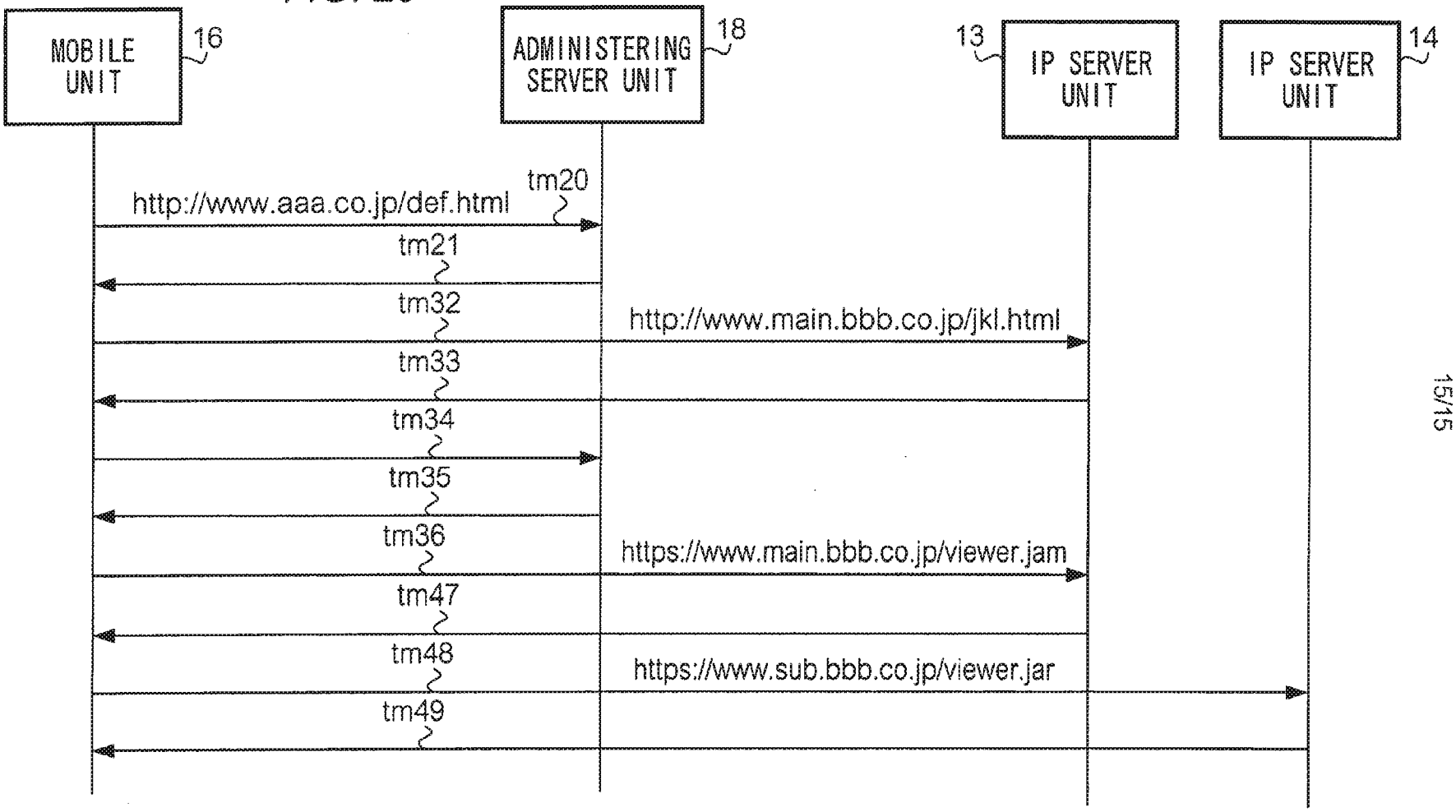

MOBILE UNIT
16
ADMINISTERING SERVER UNIT
18
12
IP SERVER UNIT
tm20
http://www.aaa.co.jp/def.html
tm21
tm32
http://www.main.bbb.co.jp/jkl.html
tm33
tm34
tm35
tm36
https://www.main.bbb.co.jp/viewer.jam
tm37
tm38
https://www.main.bbb.co.jp/viewer.jar
tm39

FIG. 19



Nintendo Exhibit 1003
Part 1 of 2
Page 00107

FIG. 20


MOBILE UNIT
16
ADMINISTERING SERVER UNIT
18
13
IP SERVER UNIT
IP SERVER UNIT
14
http://www.aaa.co.jp/def.html
tm20
tm21
tm32
http://www.main.bbb.co.jp/jkl.html
tm33
tm34
tm35
tm36
https://www.main.bbb.co.jp/viewer.jam
tm47
tm48
https://www.sub.bbb.co.jp/viewer.jar
tm49

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

82313 7590 08/17/2016

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

EXAMINER	
HESS, DANIEL A	
ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 08/17/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714	5874

TITLE OF INVENTION: SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	11/17/2016

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. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). 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. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop 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.

PTOL-85 (Rev. 02/11)

Nintendo Exhibit 1003
Part 1 of 2
Page 00109

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 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: Use Block 1 for any change of address)

82313 7590 08/17/2016
Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

Note: A certificate of mailing 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 or transmission.

Certificate of Mailing or Transmission
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 Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714	5874

TITLE OF INVENTION: SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	11/17/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
HESS, DANIEL A	2876	235-375000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ 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; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

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. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. 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 submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29
  NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27
  NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status.
  NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Nintendo Exhibit 1003
Part 1 of 2
Page 00110

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714	5874

82313 7590 08/17/2016

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

EXAMINER	
HESS, DANIEL A	

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 08/17/2016

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

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Nintendo Exhibit 1003
Part 1 of 2
Page 00111

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. 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 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. 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.

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 14/715,227	Applicant(s) ADAMS ET AL.	
	Examiner DANIEL HESS	Art Unit 2876	AIA (First Inventor to File) Status No

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

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY 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.

1. ☒ This communication is responsive to *7/27/2016 communication from applicant*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-3,5-10,12-14 and 16-23*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

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

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 4/8/2016; 7/22/2016
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/DANIEL HESS/
Primary Examiner, Art Unit 2876

DETAILED ACTION

This action is responsive to applicant's communication, including amendments and arguments, of 7/27/2016.

The present application is being examined under the pre-AIA first to invent provisions.

Allowable Subject Matter

Claims 1-3, 5-10, 12-14 and 16-23 are allowed.

The following is an examiner's statement of reasons for allowance:

The prior art of record fails to teach or fairly suggest, in the context of all other limitations present, "receiving, by the electronic device, owner control information that comprises a list of applications permitted for installation on the electronic device, and permissions associated with each permitted application in the list of applications".

The rejections the examiner has made (see for example non-final rejection of 4/27/2016) are based in large part on the access control list (ACL) such as is found in the Microsoft Windows series of operating systems.

The claims as now amended recite 'a list of applications permitted for installation' along with intended permissions for each. This is markedly different from an access control list, because the access control list is a list of permissions for current applications and other files. The access control list would not include files that are not currently on the computer, such as applications not currently installed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANIEL HESS whose telephone number is (571)272-2392. The examiner can normally be reached on 9:00 AM - 5:00 PM M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/DANIEL HESS/
Primary Examiner, Art Unit 2876

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14715227	ADAMS ET AL.
	Examiner	**Art Unit**
	DANIEL HESS	2876

CPC							
Symbol						**Type**	**Version**
G06F		21	/	6218		F	2013-01-01
G06F		12	/	1458		I	2013-01-01
G06F		21	/	51		I	2013-01-01
G06F		21	/	52		I	2013-01-01
G06F		21	/	53		I	2013-01-01
G06F		21	/	629		I	2013-01-01
G06F		21	/	71		I	2013-01-01
G06F		2221	/	2149		A	2013-01-01
H04L		63	/	102		A	2013-01-01
H04M		1	/	72525		I	2013-01-01
H04L		67	/	34		I	2013-01-01
G06F		8	/	61		I	2013-01-01
			/				
			/				
			/				

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/DANIEL HESS/ Primary Examiner.Art Unit 2876	08/11/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14715227	ADAMS ET AL.
	Examiner	**Art Unit**
	DANIEL HESS	2876

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
235	375	G 0 6 F 9 / 45 (2006.01.01)	

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
717	168	174			

NONE	Total Claims Allowed:
(Assistant Examiner) (Date)	20
/DANIEL HESS/ Primary Examiner.Art Unit 2876 08/11/2016	O.G. Print Claim(s): 1 — O.G. Print Figure: 1
(Primary Examiner) (Date)	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14715227	ADAMS ET AL.
	Examiner	**Art Unit**
	DANIEL HESS	2876

☒ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☐ **T.D.** ☐ **R.1.47**

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		20												
	2		21												
	3		22												
	5		23												
	6														
	7														
	8														
	9														
	10														
	12														
	13														
	14														
	16														
	17														
	18														
	19														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/DANIEL HESS/ Primary Examiner.Art Unit 2876 (Primary Examiner)	08/11/2016 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	4	(RFID near4 mount) with (rotat$5 or hing$4)	US-PGPUB; USPAT	OR	OFF	2015/09/03 16:49
S2	0	(RFID near4 mount) with (joint)	US-PGPUB; USPAT	OR	OFF	2015/09/03 16:54
S3	147	(RFID with mount$4) with (rotat$5 or hing$4)	US-PGPUB; USPAT	OR	OFF	2015/09/03 16:54
S4	19	(RFID with mount$4) with (hing$4)	US-PGPUB; USPAT	OR	OFF	2015/09/03 16:56
S5	156	rfid adj2 holder	US-PGPUB; USPAT	OR	OFF	2015/09/03 17:02
S6	55	S5 and rotat$5	US-PGPUB; USPAT	OR	OFF	2015/09/03 17:02
S7	17	S5 and hing$5	US-PGPUB; USPAT	OR	OFF	2015/09/03 17:06
S8	4	("20120061465" | "20120309307" | "20130206841" | "20130225079").PN.	US-PGPUB; USPAT	OR	OFF	2015/12/07 12:37
S9	1	"20120223045".did.	US-PGPUB; USPAT	OR	OFF	2015/12/07 14:20
S10	1	"20060050012".did.	US-PGPUB; USPAT	OR	OFF	2015/12/07 16:33
S11	1	"20060017573".did.	US-PGPUB; USPAT	OR	OFF	2016/01/12 16:00
S12	1	"20130206841".did.	US-PGPUB; USPAT	OR	OFF	2016/01/12 16:39
S13	6	(self adj checkout) same weight same appearance	US-PGPUB; USPAT	OR	OFF	2016/01/14 09:58
S14	1	"7036734".did.	US-PGPUB; USPAT	OR	OFF	2016/01/14 13:53
S15	1	"7036734".did.	US-PGPUB; USPAT	OR	OFF	2016/01/14 13:59
S16	1	("6,269,342" "5,271,64").did.	US-PGPUB;	OR	OFF	2016/01/15 13:17

			USPAT			
S17	2	("6,269,342" "5,271,642").did.	US-PGPUB; USPAT	OR	OFF	2016/01/15 13:18
S18	152	rfid with threaded	US-PGPUB; USPAT	OR	OFF	2016/01/15 15:36
S19	152	rfid with threaded	US-PGPUB; USPAT	OR	ON	2016/01/15 15:36
S20	5	zocca.in. and (method adj decoding).ti.	US-PGPUB; USPAT	OR	ON	2016/01/15 17:18
S21	1	"6479016".did.	US-PGPUB; USPAT	OR	ON	2016/01/19 17:43
S22	4	hess.xp. and nemet.in. and pathway.clm.	US-PGPUB; USPAT	OR	ON	2016/01/19 17:58
S23	0	hess.xp. and nemet.in. and pathwa.clm.	US-PGPUB; USPAT	OR	ON	2016/01/20 10:21
S24	0	(booster adj antenna) with (adhesive adj modification adj layer)	US-PGPUB; USPAT	OR	ON	2016/01/20 13:41
S25	5	(adhesive adj modification adj layer)	US-PGPUB; USPAT	OR	ON	2016/01/20 13:44
S26	49	rfid with adhesive with break$4	US-PGPUB; USPAT	OR	ON	2016/01/20 13:57
S27	11	rfid with adhesive with break$4 with antenna	US-PGPUB; USPAT	OR	ON	2016/01/20 13:58
S28	5	("7102520" | "7224280" | "7728734" | "7768405" | "8072333").PN.	US-PGPUB; USPAT	OR	OFF	2016/01/20 14:06
S29	6	(encode) near3 (transmissivity)	US-PGPUB; USPAT	OR	ON	2016/01/20 15:20
S30	5	("7102520" | "7224280" | "7728734" | "7768405" | "8072333").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2016/01/20 17:15
S31	1	"20130288078".did.	US-PGPUB; USPAT; USOCR	OR	OFF	2016/01/21 11:18
S33	113	S32 and helium	US-PGPUB; USPAT; USOCR	OR	OFF	2016/01/21 12:58
S34	50	S33 and deposition	US-PGPUB; USPAT; USOCR	OR	OFF	2016/01/21 12:59
S35	22	S34 and memory	US-	OR	OFF	2016/01/21

			PGPUB; USPAT; USOCR			12:59
S36	119	(magnetic same film same cryogenic$4)	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:00
S37	25	S36 and deposition and helium	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:00
S38	16	S36 and deposition and (gas near5 helium)	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:00
S39	1	"7488609".did.	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:03
S40	64	(cryogenic same (helium near4 gas) same deposition)	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:09
S41	5	(cryogenic same (cooling adj gas) same deposition)	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:10
S42	2	S41 and chuck	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:23
S43	421	cryogenic with deposition	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:49
S44	0	S43 and bifurcation	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:49
S45	0	S43 and (sealed with half)	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:49
S46	151	S43 and (sealed)	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:50
S47	3	S43 and (sealed with below)	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:50
S48	26	("20010021537" | "20020054462" | "20030091871" | "20080253024" | "20090162948" | "20090289270" | "20120164486" | "20130288078" | "4103315" | "4478877" | "5487356" | "5590389" | "5948553" | "6110542" | "6139951" | "6245451" | "6342311" | "6361627" | "6524956" | "6636460" | "6740397" | "6778358" | "6791796" | "6908517" | "8064161" | "8619394").PN.	US-PGPUB; USPAT	OR	OFF	2016/01/21 13:59
S49	0	S48 and bifurcation	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:00
S50	0	S48 and (isolated near2 half)	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:00
S51	0	S48 and (isolated near2 top)	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:00

Nintendo Exhibit 1003
Part 1 of 2
Page 00122

S52	0	S48 and (isolated near2 bottom)	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:00
S53	0	S43 and (isolated near2 bottom)	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:00
S54	0	S43 and (isolated near2 top)	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:00
S55	0	S43 and (isolated near2 half)	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:00
S56	0	S43 and (isolat$3 near2 half)	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:00
S57	0	S43 and (isolat$3 near2 top)	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:00
S58	0	S43 and (isolat$3 near2 bottom)	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:01
S59	0	(crygenic adj cooling) same bifurcation	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:04
S60	0	(crygenic adj cooling) same bifurcation	US-PGPUB; USPAT	OR	ON	2016/01/21 14:04
S61	0	(crygenic adj cooling) same (below near2 substrate)	US-PGPUB; USPAT	OR	ON	2016/01/21 14:05
S62	0	(crygenic) same (below near2 substrate)	US-PGPUB; USPAT	OR	ON	2016/01/21 14:05
S63	0	(crygenic) same (sealed near2 substrate)	US-PGPUB; USPAT	OR	ON	2016/01/21 14:05
S64	1	(cryogenic adj cooling) same bifurcation	US-PGPUB; USPAT	OR	OFF	2016/01/21 14:05
S65	3	(cryogenic adj cooling) same (below near2 substrate)	US-PGPUB; USPAT	OR	ON	2016/01/21 14:05
S66	0	(cryogenic) same (sealed near2 substrate)	US-PGPUB; USPAT	OR	ON	2016/01/21 14:06
S67	4	nemet.in. and hess.xp. and pathway.clm.	US-PGPUB; USPAT	OR	ON	2016/01/21 16:23
S68	1	"20070152039".did.	US-PGPUB; USPAT	OR	OFF	2016/08/10 08:41
S69	4	walsh.in. and declan.in. and hess.xp.	US-PGPUB; USPAT	OR	OFF	2016/08/10 11:36
S70	4	S69 and (size adj marker)	US-PGPUB; USPAT	OR	OFF	2016/08/10 11:36

S71	5	("20030209239" | "20040095746" | "20060107979" | "20100089395" | "20110041845").PN.	US-PGPUB; USPAT	OR	OFF	2016/08/10 12:54
S72	4	walsh.in. and declan.in. and hess.xp.	US-PGPUB; USPAT	OR	OFF	2016/08/10 13:31
S73	1	"4803347".did.	US-PGPUB; USPAT	OR	OFF	2016/08/10 14:24
S74	1	"6263799".did.	US-PGPUB; USPAT	OR	OFF	2016/08/10 15:41
S75	9	adams.in. and hess.xp.	US-PGPUB; USPAT	OR	OFF	2016/08/11 12:16
S76	2	S75 and (owner adj control).clm.	US-PGPUB; USPAT	OR	OFF	2016/08/11 12:16
S77	1	S76 and installation.clm.	US-PGPUB; USPAT	OR	OFF	2016/08/11 12:16
S78	1	S75 and installation.clm.	US-PGPUB; USPAT	OR	OFF	2016/08/11 12:27
S79	118	applications near2 (permitted or allowed) near2 install$6	US-PGPUB; USPAT	OR	OFF	2016/08/11 13:20
S80	331	applications near2 (permitted or allowed) near2 install$6	US-PGPUB; USPAT	OR	ON	2016/08/11 13:20
S81	11	(list near2 applications) near2 (permitted or allowed) near2 install$6	US-PGPUB; USPAT	OR	OFF	2016/08/11 13:20
S82	345	applications near2 ((white adj list) or whitelist)	US-PGPUB; USPAT	OR	OFF	2016/08/11 13:21
S83	668	applications near2 ((white adj list) or whitelist)	US-PGPUB; USPAT	OR	ON	2016/08/11 13:22

EAST Search History (Interference)

< This search history is empty>

8/ 11/ 2016 3:32:28 PM
C:\ Users\ dhess1\ Documents\ EAST\ Workspaces\ _____rfid_holder.wsp

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

	1	Canadian Office Action; Application No. 2,564,186; February 29, 2016; 4 pages. (4214-25706)

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DANIEL A HESS/	Date Considered	08/11/2016

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

X The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2016-04-08
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

	1	European Examination Report; Application No. 05741262.9; February 18, 2009; 5 pages. (4214-25709)
	2	European Examination Report; Application No. 05741262.9; April 25, 2016; 3 pages. (4214-25709)

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DANIEL A HESS/	Date Considered	08/11/2016

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2016-07-22
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14715227	ADAMS ET AL.
	Examiner	Art Unit
	DANIEL HESS	2876

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	375, 380	6/27/2015	DH
719	328		
717	168, 174		

SEARCH NOTES		
Search Notes	Date	Examiner
East keyword searches attached	6/27/2015	DH
Keyword searches updated	4/7/2016	DH
East keyword search updated	8/11/2016	DH

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
235	375, 380	8/11/2016	DH
719	328		
717	168, 174		

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method of application control on an electronic device, the method comprising:

receiving, by the electronic device, owner information from an owner of the electronic device;

receiving, by the electronic device, owner control information that ~~identifies permissions associated with applications executable by the electronic device~~comprises:

a list of applications permitted for installation on the electronic device, and

permissions associated with each permitted application in the list of applications;

storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;

determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and

controlling application access to the local memory based upon the determining.

Nintendo Exhibit 1003
Part 1 of 2
Page 00134

2. (Original) The method of claim 1, wherein the request to access the local memory comprises a request to erase data from the local memory.

3. (Original) The method of claim 1, wherein the request to access the local memory comprises a request to read data from the local memory.

4. (Canceled)

5. (Previously Presented) The method of claim 1, further comprising restricting modification of the owner control information after the owner control information has been stored in the protected data store.

6. (Previously Presented) The method of claim 1, wherein the owner control information includes an authorization record and an application identifier for each of the applications, and the owner control information is provided by an external source through a wireless communication channel.

7. (Previously Presented) The method of claim 6, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

8. (Previously Presented) The method of claim 1, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

9. (Original) The method of claim 1, wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device, the method further comprising:

receiving requests to access the local memory from a plurality of applications operating on the electronic device;

determining whether access to the local memory is allowed to be performed by their respective applications based upon the stored authorization records and the application identifiers that are respectively associated with the plurality of applications; and

controlling access by the plurality of applications to local memory based upon whether access to the local memory is allowed.

10. (Original) The method of claim 9, wherein a group containing two or more of the applications is associated with one of the authorization records.

11. (Canceled)

Nintendo Exhibit 1003
Part 1 of 2
Page 00136

12. (Currently Amended) A device, comprising:

a memory; and

a processor coupled with the memory and configured by instructions stored in the memory to:

receive owner information from an owner of the device;

receive owner control information that ~~identifies permissions associated with applications executable by the device~~comprises:

a list of applications permitted for installation on the device, and

permissions associated with each permitted application in the list of applications;

store the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receive, from an application operating on the electronic device, a request to access local memory on the electronic device;

determine whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and

control application access to the local memory based upon the determining.

13. (Original) The device of claim 12, wherein the request to access the local memory comprises a request to erase data from the local memory.

Nintendo Exhibit 1003
Part 1 of 2
Page 00137

14. (Original) The device of claim 12, wherein the request to access the local memory comprises a request to read data from the local memory.

15. (Canceled)

16. (Previously Presented) The device of claim 12, further comprising restricting modification of the owner control information after the owner control information has been stored on the electronic device.

17. (Previously Presented) The device of claim 12, wherein the owner control information includes an authorization record and an application identifier for each of the applications, and wherein the owner control information is provided by an external source through a wireless communication channel.

18. (Previously Presented) The device of claim 17, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

19. (Previously Presented) The device of claim 12, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

Nintendo Exhibit 1003
Part 1 of 2
Page 00138

20. (Currently Amended) A non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the operations of:

receiving owner information from an owner of an electronic device;

receiving owner control information that ~~identifies permissions associated with applications executable by the electronic device~~comprises:

a list of applications permitted for installation on the electronic device, and

permissions associated with each permitted application in the list of applications;

storing the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receiving, from an application operating on the electronic device, a request to access local memory on the electronic device;

determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and

controlling application access to the local memory based upon the determining.

21. (Previously Presented) The non-transitory computer-readable medium of claim 20, wherein the owner control information includes an authentication record and an identifier for each application allowed to be executed on the electronic device.

22. (Previously Presented) The non-transitory computer-readable medium of claim 20, wherein the request to access the local memory comprises a request to erase data from the local memory.

23. (Previously Presented) The non-transitory computer-readable medium of claim 20, wherein the request to access the local memory comprises a request to read data from the local memory.

Nintendo Exhibit 1003
Part 1 of 2
Page 00140

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: BlackBerry Limited	§	
	§	Group Art Unit: 2876
Application No.: 14/715,227	§	
	§	Examiner: Daniel A. Hess
Filed: May 18, 2015	§	
	§	Confirmation No.: 5874
For: SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES	§	

AMENDMENT AND RESPONSE TO
OFFICE ACTION DATED APRIL 27, 2016

Commissioner:

In response to the Office Action dated April 27, 2016 in the above-identified application, the Applicant respectfully submits the following Amendment and Response. The changes made are shown by underlining the added text and striking through or double-bracketing the deleted text.

Amendments to the Claims are reflected in the listing of claims that begins on Page 2 of this paper.

Remarks begin on Page 9 of this paper.

Electronic Acknowledgement Receipt

EFS ID:	26473179
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Lesley Forte
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	27-JUL-2016
Filing Date:	18-MAY-2015
Time Stamp:	17:03:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		11913-US-CNT3_2016-07-27_RESP_OA3.pdf	80689 c6ac49b2e96526c5c6bb43d5e6d538cc1dab7187	yes	14

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	14
Warnings:			
Information:			
	Total Files Size (in bytes):	80689	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

REMARKS

The Office Action of April 27, 2016 has been carefully reviewed. The Applicant respectfully requests the Examiner to reconsider the rejections and allow the pending claims in view of the following remarks.

STATUS OF CLAIMS

Claims 1-3, 5-10, 12-14 and 16-23 stand rejected. Claims 4, 11 and 15 were previously canceled. Claims 1, 12, and 20 are hereby amended. Support for these amendments may be found in at least paragraph 24 of the specification. No new matter has been added.

INFORMATION DISCLOSURE STATEMENT

The Applicant respectfully requests confirmation in the next communication from the Office that the Applicant's IDS filed on April 8, 2016 has been received and considered by the Examiner.

REJECTION OF CLAIMS – 35 U.S.C. § 103

In the Office Action mailed April 27, 2016, the Examiner rejected claims 1-3, 5-10, 12-14, and 16-23 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2003/0101292 to Fisher, et al. ("Fisher") in view of U.S. Patent No. 5,761,669 to Montague, et al. ("Montague").

For convenience, the Applicant will address the claims at issue with respect to claim 1. Claim 1, as amended, recites:

> 1. A method of application control on an electronic device, the method comprising:
>
> receiving, by the electronic device, owner information from an owner of the electronic device;
>
> **receiving, by the electronic device, owner control information that comprises:**
>
> **a list of applications permitted for installation on the electronic device, and**
>
> **permissions associated with each permitted application in the list of applications;**
>
> storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;
>
> receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;
>
> determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and
>
> controlling application access to the local memory based upon the determining.

(Emphasis added). The Applicant submits that the cited prior art does not disclose at least the elements of amended claim 1 emphasized above.

The Office Action alleges that "Fisher shows the principle whereby multiple users on a computer system and the applications associated with that user are granted access to certain local memory and barred access to other local memory." Office Action at p. 4. Fisher discloses that "to permit multiple users to access a single computer system, the various users (and their applications) are assigned various separate resources within the system." Fisher, ¶ 4. Specifically, Fisher discloses that "various memory addresses are assigned to one user application and various other memory addresses are assigned to another to avoid overlap" and "interference between applications." *Id.*

However, Fisher does not receive owner control information that comprises a list of applications permitted for installation on the electronic device and permissions associated

with each permitted application in the list of applications as claimed. Instead, Fisher generally discloses the idea of an intermediary dynamic execution layer interface (DELI) that resides between an application and a hardware layer to untie binary code of the application from the hardware layer. *Id.* at ¶ 19. In addition, Fisher discloses that "Generally speaking, irrespective of whether the DELI 100 has gained *control over the execution of the application 102* transparently or nontransparently, the application does not execute directly on the hardware 104. Rather, *application code executes through the DELI 100....*" *Id.* at ¶ 47. Therefore, Fisher discloses operations that occur when an application is **executing**, but is silent with respect to controlling what applications are installed on the device prior to attempted execution. Consequently, while Fisher discloses the idea of controlling execution of an application installed on a device by using an intermediary layer, Fisher does not receive owner control information that comprises a list of applications permitted for installation on the electronic device and permissions associated with each permitted application in the list of applications as claimed.

Montague discloses that an access control list may be used to indicate users for which access control rights can be set with regard to software or hardware controlled by a server. *See* Montague at col. 7, ll. 27-33 and col. 1, ll. 23-27. Montague further discloses that a user determines a software or hardware component to be restricted, and access rights to be applied to the software or hardware component. *See id.* at col. 6, ll. 39-58 and Abstract. However, Montague does not receive owner control information that comprises a list of applications permitted for installation on the electronic device and permissions associated with each permitted application in the list of applications as claimed:

> **The present invention is a set of routines for controlling access to certain entities on a network in a manner that does not require a user to identify the appropriate server and does not require that the user know the format for setting access permissions in the operating system running on that server.** The routines comprising the present invention can either be part of a network operating system, integrated into or accessed from an application, or may be provided as separate stand-alone application on a network. Generally, the routines enable a user to identify a specific entity for which access rights are to be set or modified. **The routines, not the user, will determine the server that controls a specific entity. Once the user selects the entity, the trustee, and indicates the access rights to be applied, the routines will determine if the user has the right to set the requested permissions and whether the trustee has the required permissions relative to the entity, and if so, will convert the user's request into the appropriate format and function calls implemented in the operating system running on the server that controls the entity.**
>
> **Conceptually, each operating system/server maintains some form of persistent database that specifies each trustee for which access rights can be set in regard to any entity controlled or associated with the server and a data structure that specifies requisite access controls.** In the WINDOWS NT operating system, the database is called an "access control list" (ACL), but other types of data structures can also be used for this purpose.

Montague, col. 6, ll. 39-58, col. 7, ll. 27-33 (emphasis added). As shown above, Montague controls access to software or hardware components in a network according to entries in an access control list. *See id.* In other words, Montague merely teaches that an administrator may limit a user's access to software or hardware components operating in the network. *See id.* However, Montague fails to disclose receiving owner control information that comprises a list of applications permitted for installation on the electronic device and permissions associated with each permitted application in the list of applications. Indeed, Montague is wholly unrelated to, and completely silent with respect to, controlling which applications are installed on an electronic device. *See id.* at Abstract. Instead, Montague is focused on controlling user access to software or

hardware on a network through permissions set on a server on the network. *See id.* Therefore, Montague does not receive owner control information that comprises a list of applications permitted for installation on the electronic device and permissions associated with each permitted application in the list of applications as claimed. As such, Montague does not cure the deficiencies of Fisher.

Therefore, claim 1, as amended, is not rendered obvious by the combination of Fisher and Montague. Claims 12 and 20, as amended, recite similar elements to amended claim 1. Therefore, claims 12 and 20 are likewise not rendered obvious by the combination of Fisher and Montague. For at least the foregoing reasons, the Applicant respectfully requests the Examiner to reconsider and withdraw the rejections of claims 1, 12, 20, and their dependent claims.

Nintendo Exhibit 1003
Part 1 of 2
Page 00148

CONCLUSION

The Applicant respectfully submits that the application, in its present form, is in condition for allowance. If the Examiner has any questions or comments or otherwise feels it would be helpful in expediting the application, the Examiner is encouraged to telephone the undersigned at (972) 731-2288. The Applicant intends this communication to be a complete response to the Office Action mailed April 27, 2016.

The Commissioner is hereby authorized to charge payment of any fee associated with any of the foregoing papers submitted herewith or any fees during the prosecution of the present case to Deposit Account No. 50-1515, Conley Rose, P.C.

Respectfully submitted,

CONLEY ROSE, P.C.

Date: July 27, 2016

/J. Robert Brown, Jr./
J. Robert Brown, Jr.
Reg. No. 45,438

ATTORNEY FOR APPLICANT

5601 Granite Parkway, Suite 500
Plano, Texas 75024
Telephone: (972) 731-2288
Facsimile: (972) 731-2289

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
14/715,227	05/18/2015	

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	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 $310 ($155 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))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **07/27/2016**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					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.

LIE
ANDREA FREEMAN

This collection of information is required by 37 CFR 1.16. 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 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Patent Application Fee Transmittal

Application Number:	14715227
Filing Date:	18-May-2015
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	J. Robert Brown/Rami Law
Attorney Docket Number:	11913-US-CNT3 4214-25714

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	26425815
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Rami Law
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	22-JUL-2016
Filing Date:	18-MAY-2015
Time Stamp:	15:17:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$180
RAM confirmation Number	072516INTEFSW00001707501515
Deposit Account	501515
Authorized User	Rami Law
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	11913-US-CNT3_2016-07-22_IDS.pdf	614655 92e3eb43c238d66b25a908edd86e990283578ca	no	4
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Other Reference-Patent/App/Search documents	EPExam_25709_021809.pdf	427966 12a959b452636367a678563ad7f67c3efac3bd21	no	5
Warnings:					
Information:					
3	Other Reference-Patent/App/Search documents	EPExam_25709_042516.pdf	299078 046c1832ff51292e651189560f087b20bed6fd5a	no	3
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30811 398c7c13ca27c27a26642df985e80d7e16e30ff4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1372510		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14715227
	Filing Date	2015-05-18
	First Named Inventor	Neil P. Adams
	Art Unit	2876
	Examiner Name	Daniel A. Hess
	Attorney Docket Number	11913-US-CNT3 4214-25714

	1	European Examination Report; Application No. 05741262.9; February 18, 2009; 5 pages. (4214-25709)
	2	European Examination Report; Application No. 05741262.9; April 25, 2016; 3 pages. (4214-25709)

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2016-07-22
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2004053618	WO	A2	2004-06-24	Research In Motion Limited		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

	1	HOUSLEY, R., et al.; "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"; RFC 2459; January 1999; 129 pages.
	2	European Summons to Attend Oral Proceedings; Application No. 05739066.8; October 30, 2015; 6 pages. (4214-25708)

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DANIEL A HESS/	Date Considered	04/07/2016

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2016-01-25
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.A.H/

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of References Cited	Application/Control No. 14/715,227	Applicant(s)/Patent Under Reexamination ADAMS ET AL.	
	Examiner DANIEL HESS	Art Unit 2876	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,761,669 A	06-1998	Montague; David S.	G06F21/604	707/758
	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	CPC 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.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14715227	ADAMS ET AL.
	Examiner	**Art Unit**
	DANIEL HESS	2876

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/27/2015	11/03/2015	04/07/2016						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	-	-						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	-						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	-	-						
	16	✓	✓	✓						
	17	✓	✓	✓						
	18	✓	✓	✓						
	19	✓	✓	✓						
	20	✓	✓	✓						
	21			✓						
	22			✓						
	23			✓						

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714	5874

82313 7590 04/27/2016

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

EXAMINER	
HESS, DANIEL A	

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
04/27/2016	ELECTRONIC

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

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

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

ConleyRoseReporting@dfw.conleyrose.com

Office Action Summary	Application No. 14/715,227	Applicant(s) ADAMS ET AL.	
	Examiner DANIEL HESS	Art Unit 2876	AIA (First Inventor to File) Status No

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

Period for Reply

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

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

Status

1)☒ Responsive to communication(s) filed on *2/10/2016*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

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

Disposition of Claims*

5)☒ Claim(s) *1-3,5-10,12-14 and 16-23* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-3,5-10,12-14 and 16-23* is/are rejected.

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

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

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

Application Papers

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

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

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *1/25/2016*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

This action is responsive to applicant's pre-appeal conference request of 2/10/2016. The pre-appeal conference occurred on 4/5/2016, and the decision was to reopen prosecution. The conferees were SPE David Martin and SPE Michael G. Lee.

Response to Pre-Appeal Conference Request

In the pre-appeal conference request of 2/10/2016, the applicant particularly questioned the Windows XP Guide reference, writing, in part:

"However, the Applicant submits that relying on Windows XP Guide as allegedly teaching the claimed features is improper because Windows XP Guide does not constitute prior art with respect to the present application. The present application claims priority to a U.S. provisional application No. 60/432,610 filed on December 12, 2002, which predates the publication date of Windows XP Guide, which is November 3, 2005. See MPEP § 706."

The examiner argued in the pre-appeal conference that Windows XP Guide, although published in 2005, is a user guide for a product (Windows XP) that was released in 2001. However the conferees in the pre-appeal conference agreed with the applicant that the reference is inadmissible because of its later publication date. (One conferee noted that there could for example be different versions of Windows XP and the Windows XP Guide could describe features released in a later version).

Therefore, the examiner herewith introduces a new reference, Montague et al. (US 5,761,669), assigned to Microsoft Corporation and filed in 1995. Montague et al. (see for example figures 4 and 6; column 2, lines 4-17; column 7, lines 25-35; column 8, lines 44-55; column 9) teaches Access Control Lists in Windows, the concept of read and write permissions grantable to different users, and the concept of ownership. The examiner maintains that Montague et al. is consistent with the teachings of Windows XP Guide, but has the benefit of a publication date that is more than ten years earlier.

Claim Rejections - 35 USC § 103

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

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

Claims 1-3, 5-10, 12-14 and 16-23 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Fisher et al. (US 2003/0101292) in view of Montague et al. (US 5,761,669).

Re claim 1, 5:

Fisher applies to an electronic device.

Fisher teachs at para [0004]:

"**In order to permit multiple users to access a single computer system, the various users (and their applications) are assigned various separate resources within the system.** For instance, **various memory addresses are**

assigned to one user application and various other memory addresses are assigned to another to avoid overlap. This is known in the art as sandboxing. Such separation is used to avoid interference between applications that can cause undesired effects to occur."

Fisher teaches at para [0006]:

"**Substantially all multiprogrammed systems rely upon software and/or hardware solutions that prevent applications from accessing memory addresses that are out of the permissible range.** The software solutions typically at least statically review the instructions of a particular application when it is loaded to determine whether any of the instructions contain a direct memory reference to an out-of-range memory address."

Fisher shows the principle whereby multiple users on a computer system and the applications associated with that user are granted access to certain local memory and barred access to other local memory. This achieves several ends as the above excerpt demonstrates:

(1) Memory can be allocated to users and their applications can only use the memory that belongs to their owners.

(2) A first application cannot access and interfere with the memory of a second different application, possibly by a different user.

In keeping with the above, application identifiers would be associated with user identifiers and memory is associated with user identifiers. Users of a system in turn would have their own authorizations to be able to access the system and applications gain authorization to access certain memory through those users.

It is noted that this principle of delineated memory seen above applies both on a larger level to user accounts and on a finer level to multiple applications belonging to the same user.

"Insertion of additional owner information" would be restricted at least in the sense that another user on the same level could not on their own obtain access to memory and applications belonging to a different user. That is the meaning of assigning users control. See discussions above.

Regarding the teachings of Montague et al., (see for example figures 4 and 6; column 2, lines 4-17; column 7, lines 25-35; column 8, lines 44-55; column 9), the underlying operating system (in this instance Windows, the most widespread operating system in the world) is governed by an access control list (ACL). Every file in the ACL has (see for instance figures 4 and 6) an entry associated with it that governs access permissions for that file, and this would include every application. The entry for a particular application governs permissions for that application. The Access Control List (ACL) is a Windows operating system file which is protected. Another user that is not the owner of a file may not have access unless granted by the owner. As figure 4 shows, another user other than the owner can have various access levels including read access, write access, or no access depending on permissions granted by an owner

or administrator. Access Control Lists show how some users are walled off from accessing files (including applications) belonging to other users.

In view of the teachings of Montague et al., it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the file access control system based on owners and access control lists and file permissions as per Montague et al. because every operating system needs to control which users have what kind of access to which files in a permanent and protected way. This is the way of Windows, the world's dominant operating system at the time of the invention and at the time of this writing. Indeed, Fisher probably already has this type of underlying operating system (but since one cannot know for sure, a secondary reference is applied).

The examiner asserts that the claims are a combination of owner access control through protected files (as per Montague et al.'s teaching), in order to determine whether a user/owner can access a program at all, and then determining whether the program is allowed to access a particular section of memory (as per the memory sandboxing of Fisher).

Re claims 2 and 3: Memory access by an application as described above generally includes all of read, write and erase ability.

Re claim 6: See para 0039, where it is seen that the system in question can be a server computer. Server computers are conventionally accessed remotely for both control and providing service to clients. Wireless networks could reasonably be part of the remote access configuration in Fisher et al.

Re claims 7 and 8: Claims 1 and 7 to a good approximation describe the configuration that has been present at the USPTO since prior to the instant invention. An external server system managed by the USPTO administers all policies. Specifically the server supplies users with access to applications and pushes applications for users. Users have specifically allocated memory on servers for their accounts and to be used by their application.

This is similar to what is seen in paragraphs 0004 and 0006 of Fisher, but with organizational control.

Re claims 9 and 10: Fisher clearly can apply (as seen in the excerpt above) to user accounts that may have multiple applications in them. The authorization record, which is associated with one user, applies to two or more applications.

Re claim 11: In the case of organization controlled IT, described above, regular users may not install or delete any application within their allocated space. This an administrative-level function. Users certainly can run applications and operate within applications to create and delete data files associated with those applications, but they may not control the installation and authorizations of applications. This is a protected data store.

Re claims 12-14, 16: See discussions re claims 1-3, above.

Re claims 17-19: See discussion re claims 6-8, above.

Re claim 20: See discussion re claim 1 above.

Re claim 21: See figures 4 and 6 of Montague et al. which show the file permissions for a single file, which represents a single record in the Access Control List of the operating system.

A similar record would exist for every application, since an application is also a type of file. The identifier is the name of the application file, and the authentication record are the permissions.

Re claim 22: A request to erase data falls in the category of write permissions. Write permissions are one of the things that is governed by the Access Control List and File Permissions disclosed in Montague et al.

Also, overall access to particular memory by a particular application is controlled as seen in Fisher et al. Specific applications are allowed to operate only in specific memories.

Re claim 23: A request to read data falls in the category of read permissions. Read permissions are one of the things that is governed by the Access Control List and File Permissions disclosed in Montague et al.

Also, overall access to particular memory by a particular application is controlled as seen in Fisher et al. Specific applications are allowed to operate only in specific memories.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANIEL HESS whose telephone number is (571)272-2392. The examiner can normally be reached on 9:00 AM - 5:00 PM M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/DANIEL HESS/
Primary Examiner, Art Unit 2876

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14715227	ADAMS ET AL.
	Examiner	Art Unit
	DANIEL HESS	2876

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	375, 380	6/27/2015	DH
719	328		

SEARCH NOTES		
Search Notes	Date	Examiner
East keyword searches attached	6/27/2015	DH
Keyword searches updated	4/7/2916	DH

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714	5874

82313 7590 04/19/2016

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

EXAMINER	
HESS, DANIEL A	

ART UNIT	PAPER NUMBER
2876	

MAIL DATE	DELIVERY MODE
04/19/2016	PAPER

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

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

Notice of Panel Decision from Pre-Appeal Brief Review	Application No. 14/715,227	Applicant(s) ADAMS ET AL.
	Examiner DANIEL HESS	Art Unit 2876

This is in response to the Pre-Appeal Brief Request for Review filed 10 February, 2016.

1. ☐ **Improper Request** – The Request is improper and a conference will not be held for the following reason(s):

☐ The Notice of Appeal has not been filed concurrent with the Pre-Appeal Brief Request.
☐ The request does not include reasons why a review is appropriate.
☐ A proposed amendment is included with the Pre-Appeal Brief request.
☐ Other: .

The time period for filing a response continues to run from the receipt date of the Notice of Appeal or from the mail date of the last Office communication, if no Notice of Appeal has been received.

2. ☐ **Proceed to Board of Patent Appeals and Interferences** – A Pre-Appeal Brief conference has been held. The application remains under appeal because there is at least one actual issue for appeal. Applicant is required to submit an appeal brief in accordance with 37 CFR 41.37. The time period for filing an appeal brief will be reset to be one month from mailing this decision, or the balance of the two-month time period running from the receipt of the notice of appeal, whichever is greater. Further, the time period for filing of the appeal brief is extendible under 37 CFR 1.136 based upon the mail date of this decision or the receipt date of the notice of appeal, as applicable.

☐ The panel has determined the status of the claim(s) is as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: _____.
Claim(s) withdrawn from consideration: _____.

3. ☐ **Allowable application** – A conference has been held. The rejection is withdrawn and a Notice of Allowance will be mailed. Prosecution on the merits remains closed. No further action is required by applicant at this time.

4. ☒ **Reopen Prosecution** – A conference has been held. The rejection is withdrawn and a new Office action will be mailed. No further action is required by applicant at this time.

All participants:

(1) *DANIEL HESS*.	(3) *David Martin*.
(2) *Michael G. Lee*.	(4)_____.

/DANIEL HESS/ Primary Examiner, Art Unit 2876	/David S. Martin/ RQAS OPQA	/MICHAEL G LEE/ Supervisory Patent Examiner, Art Unit 2876

Electronic Patent Application Fee Transmittal

Application Number:	14715227
Filing Date:	18-May-2015
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	J. Robert Brown/Rami Law
Attorney Docket Number:	11913-US-CNT3 4214-25714

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14715227
	Filing Date	2015-05-18
	First Named Inventor	Neil P. Adams
	Art Unit	2876
	Examiner Name	Daniel A. Hess
	Attorney Docket Number	11913-US-CNT3 4214-25714

	1	Canadian Office Action; Application No. 2,564,186; February 29, 2016; 4 pages. (4214-25706)

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2016-04-08
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	25435167
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Rami Law
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	08-APR-2016
Filing Date:	18-MAY-2015
Time Stamp:	12:25:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	9316
Deposit Account	501515
Authorized User	BROWN, J. ROBERT

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	11913-US-CNT3_2016-04-08_IDS.pdf	614643 cd342f9ee886db62f62f5aa9981ae9bf9b091162	no	4
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Other Reference-Patent/App/Search documents	CAOfficeAction_25706_022916.pdf	430810 8fb2182c84fc660376707d3910c2d00a5cef10f9	no	4
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30811 cacec274087070e9988c08dbf207e534a2afdccf	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1076264		

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

Doc code: Oath
Document Description: Oath or declaration filed

PTO/AIA/02 (07-13)
Approved for use through 04/30/2017. OMB 0651-0032
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.

SUBSTITUTE STATEMENT IN LIEU OF AN OATH OR DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (35 U.S.C. 115(d) AND 37 CFR 1.64)

Title of Invention	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES

This statement is directed to:

☐ The attached application.

OR

☒ United States application or PCT international application number 14/715227 filed on 18 May 2015.

LEGAL NAME of inventor to whom this substitute statement applies:

(*E.g.*, Given Name (first and middle (if any)) and Family Name or Surname)

Michael G. Kirkup

Residence (except for a deceased or legally incapacitated inventor):

City	State	Country
Waterloo	ON	Canada

Mailing Address (except for a deceased or legally incapacitated inventor):

224 Dearborn Blvd.

City	State	Zip	Country
Waterloo	ON	N2J 4Y3	Canada

I believe the above-named inventor or joint inventor to be the original inventor or an original joint inventor of a claimed invention in the application.

The above-identified application was made or authorized to be made by me.

I hereby acknowledge that any willful false statement made in this statement is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

Relationship to the inventor to whom this substitute statement applies:

- ☐ Legal Representative (for deceased or legally incapacitated inventor only).
- ☐ Assignee.
- ☒ Person to whom the inventor is under an obligation to assign.
- ☐ Person who otherwise shows a sufficient proprietary interest in the matter (petition under 37 CFR 1.46 is required), or
- ☐ Joint Inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute 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/AIA/02 (97-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

SUBSTITUTE STATEMENT

Circumstances permitting execution of this substitute statement:

- ☐ Inventor is deceased.
- ☐ Inventor is under legal incapacity.
- ☒ Inventor cannot be found or reached after diligent effort, or
- ☐ Inventor has refused to execute the oath or declaration under 37 CFR 1.63.

If there are joint inventors, please check the appropriate box below:

- ☒ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) naming the entire inventive entity has been or is currently submitted.

OR

- ☐ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) has not been submitted. Thus, a Substitute Statement Supplemental Sheet (PTO/AIA/11 or equivalent) naming the entire inventive entity and providing inventor information is attached. See 37 CFR 1.64(b).

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.

PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

Name: Keith Bennett | Date (Optional):

Signature:

APPLICANT NAME AND TITLE OF PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

If the applicant is a juristic entity, list the applicant name and the title of the signer.

Applicant Name: BlackBerry Limited

Title of Person Executing This Substitute Statement: Authorized Signing Officer

The signer, whose title is supplied above, is authorized to act on behalf of the applicant.

Residence of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent):

City: Waterloo | State: ON | Country: Canada

Mailing Address of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent)

2200 University Avenue East

City: Waterloo | State: ON | Zip: N2K 0A7 | Country: Canada

Note: Use an additional PTO/AIA/02 form for each inventor who is deceased, legally incapacitated, cannot be found or reached after diligent effort, or has refused to execute the oath or declaration under 37 CFR 1.63.

Legal OK

Nintendo Exhibit 1003
Part 1 of 2
Page 00188

Attorney Docket No.: 11913-US-CNT[3]
4214-25714

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: BlackBerry Limited	§	Group Art Unit: 2876
	§	
Application No.: 14/715,227	§	Examiner: Daniel A. Hess
	§	
Filed: May 18, 2015	§	Confirmation No.: 5874
	§	
For: SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES	§	

RESPONSE TO INFORMATIONAL NOTICE TO APPLICANT

Commissioner:

In response to the Informational Notice to Applicant mailed June 1, 2015 in the above-referenced matter, the Applicant respectfully submits the enclosed executed Declaration and Substitute Statements.

The payment for the enclosed documents was previously submitted on May 18, 2015. However, the Commissioner is hereby authorized to charge payment of any further fees associated with any of the foregoing papers submitted herewith, or to credit any overpayment thereof, to Deposit Account No. 50-1515, Conley Rose, P.C.

Respectfully submitted,
CONLEY ROSE, P.C.

Date: March 24, 2016

/J. Robert Brown, Jr./
J. Robert Brown, Jr.
Reg. No. 45,438

ATTORNEY FOR APPLICANT

5601 Granite Parkway, Suite 500
Plano, Texas 75024
Telephone: (972) 731-2288
Facsimile: (972) 731-2289

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
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.

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

Title of Invention	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

■ United States application or PCT international application number 14/715227 filed on 18 May 2015

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

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.

LEGAL NAME OF INVENTOR

Inventor: Neil Patrick ADAMS Date (Optional): Jan 4/2016

Signature: N P A

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Doc code: Oath
Document Description: Oath or declaration filed

PTO/AIA/82 (07-13)
Approved for use through 04/30/2017. OMB 0651-0032
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.

SUBSTITUTE STATEMENT IN LIEU OF AN OATH OR DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (35 U.S.C. 115(d) AND 37 CFR 1.64)

Title of Invention	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES

This statement is directed to:

☐ The attached application.

OR

☒ United States application or PCT international application number 14/715227 filed on 18 May 2015

LEGAL NAME of inventor to whom this substitute statement applies:

(E.g., Given Name (first and middle (if any)) and Family Name or Surname)

Russell N. Owen

Residence (except for a deceased or legally incapacitated inventor):

City	State	Country
Waterloo	ON	Canada

Mailing Address (except for a deceased or legally incapacitated inventor):

450 Chesapeake Drive

City	State	Zip	Country
Waterloo	ON	N2K 4B8	Canada

I believe the above-named inventor or joint inventor to be the original inventor or an original joint inventor of a claimed invention in the application.

The above-identified application was made or authorized to be made by me.

I hereby acknowledge that any willful false statement made in this statement is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

Relationship to the inventor to whom this substitute statement applies:

- ☐ Legal Representative (for deceased or legally incapacitated inventor only).
- ☐ Assignee.
- ☒ Person to whom the inventor is under an obligation to assign.
- ☐ Person who otherwise shows a sufficient proprietary interest in the matter (petition under 37 CFR 1.46 is required), or
- ☐ Joint Inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute 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/AIA/02 (67-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

SUBSTITUTE STATEMENT

Circumstances permitting execution of this substitute statement:

- ☐ Inventor is deceased.
- ☐ Inventor is under legal incapacity.
- ☒ Inventor cannot be found or reached after diligent effort, or
- ☐ Inventor has refused to execute the oath or declaration under 37 CFR 1.63.

If there are joint inventors, please check the appropriate box below:

- ☒ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) naming the entire inventive entity has been or is currently submitted.

OR

- ☐ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) has not been submitted. Thus, a Substitute Statement Supplemental Sheet (PTO/AIA/11 or equivalent) naming the entire inventive entity and providing inventor information is attached. See 37 CFR 1.64(b).

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.

PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

Name: Keith Barnett

Date (Optional):

Signature:

APPLICANT NAME AND TITLE OF PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

If the applicant is a juristic entity, list the applicant name and the title of the signer:

Applicant Name: BlackBerry Limited

Title of Person Executing This Substitute Statement: Authorized Signing Officer

The signer, whose title is supplied above, is authorized to act on behalf of the applicant.

Residence of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent):

City: Waterloo | State: ON | Country: Canada

Mailing Address of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent)

2200 University Avenue East

City: Waterloo | State: ON | Zip: N2K 0A7 | Country: Canada

Note: Use an additional PTO/AIA/02 form for each inventor who is deceased, legally incapacitated, cannot be found or reached after diligent effort, or has refused to execute the oath or declaration under 37 CFR 1.63.

Legal OK

Nintendo Exhibit 1003
Part 1 of 2
Page 00193

Doc code: Oath
Document Description: Oath or declaration filed

PTO/AIA/02 (07-13)
Approved for use through 04/30/2017. OMB 0651-0032
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.

SUBSTITUTE STATEMENT IN LIEU OF AN OATH OR DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (35 U.S.C. 115(d) AND 37 CFR 1.64)

Title of Invention	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES

This statement is directed to:

☐ The attached application.

OR

☒ United States application or PCT international application number 14/715227 filed on 18 May 2015

LEGAL NAME of inventor to whom this substitute statement applies:

(E.g., Given Name (first and middle (if any)) and Family Name or Surname)

Herbert A. Little

Residence (except for a deceased or legally incapacitated inventor):

City	State	Country
Waterloo	Ontario	Canada

Mailing Address (except for a deceased or legally incapacitated inventor):

504 Old Oak Place

City	State	Zip	Country
Waterloo	Ontario	N2T 2V8	Canada

I believe the above-named inventor or joint inventor to be the original inventor or an original joint inventor of a claimed invention in the application.

The above-identified application was made or authorized to be made by me.

I hereby acknowledge that any willful false statement made in this statement is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

Relationship to the inventor to whom this substitute statement applies:

- ☐ Legal Representative (for deceased or legally incapacitated inventor only).
- ☒ Assignee.
- ☐ Person to whom the inventor is under an obligation to assign.
- ☐ Person who otherwise shows a sufficient proprietary interest in the matter (petition under 37 CFR 1.46 is required), or
- ☐ Joint Inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute 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/AIA/02 (07-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

SUBSTITUTE STATEMENT

Circumstances permitting execution of this substitute statement:

- ☐ Inventor is deceased.
- ☐ Inventor is under legal incapacity.
- ☒ Inventor cannot be found or reached after diligent effort, or
- ☐ Inventor has refused to execute the oath or declaration under 37 CFR 1.63.

If there are joint inventors, please check the appropriate box below:

- ☒ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) naming the entire inventive entity has been or is currently submitted.

OR

- ☐ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) has not been submitted. Thus, a Substitute Statement Supplemental Sheet (PTO/AIA/11 or equivalent) naming the entire inventive entity and providing inventor information is attached. See 37 CFR 1.64(b).

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.

PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

Name: Kevin Bennett | Date (Optional):

Signature:

APPLICANT NAME AND TITLE OF PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

If the applicant is a juristic entity, list the applicant name and the title of the signer:

Applicant Name: BlackBerry Limited

Title of Person Executing This Substitute Statement: Authorized Signing Officer

The signer, whose title is supplied above, is authorized to act on behalf of the applicant.

Residence of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent):

City: Waterloo | State: Ontario | Country: Canada

Mailing Address of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent)

2200 University Avenue East

City: Waterloo | State: Ontario | Zip: N2K 0A7 | Country: Canada

Note: Use an additional PTO/AIA/02 form for each inventor who is deceased, legally incapacitated, cannot be found or reached after diligent effort, or has refused to execute the oath or declaration under 37 CFR 1.63.

Legal OK
JLH

Electronic Acknowledgement Receipt

EFS ID:	25296168
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Lesley Forte
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	24-MAR-2016
Filing Date:	18-MAY-2015
Time Stamp:	14:20:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	11913-US-CNT3_2016-03-24_RESP_Informational_Notice.pdf	31241 93b30bf7aca57888ca87193e8152bb1a8371673a	no	1

Warnings:	
Information:	

2	Oath or Declaration filed	11913-US-CNT3_2016-03-24_SUB_DEC_Adams.pdf	159304 131a8ff98b5e12f8b0e1a02f049419e55db27319	no	2
Warnings:					
Information:					
3	Oath or Declaration filed	11913-US-CNT3_2016-03-24_SUB_DEC_SS_Kirkup.pdf	525239 0523ab96982b470c349ffc9460f162188ce414e8	no	2
Warnings:					
Information:					
4	Oath or Declaration filed	11913-US-CNT3_2016-03-24_SUB_DEC_SS_Little.pdf	538919 6604e5bc36c6c86a81d019f52f2d0968f2e4a887	no	2
Warnings:					
Information:					
5	Oath or Declaration filed	11913-US-CNT3_2016-03-24_SUB_DEC_SS_Owen.pdf	529560 49ad4f3b549b1afab63811a14bc51e80492fa06b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1784263		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Electronic Acknowledgement Receipt

EFS ID:	24882018
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Judy Fan
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	10-FEB-2016
Filing Date:	18-MAY-2015
Time Stamp:	17:35:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$800
RAM confirmation Number	4261
Deposit Account	501515
Authorized User	BROWN, J. ROBERT

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Notice of Appeal Filed	11913-US-CNT3_2016-02-10_RESP_OA2_AA_Notice_of_Appeal.pdf	244502 13f096da1b6bd292d094d5c86bc7a90cbf7ce964	no	2
Warnings:					
Information:					
2	Pre-Brief Conference request	11913-US-CNT3_2016-02-10_RESP_OA2_AA_Pre-Appeal_Brief.pdf	219461 46232abe8ad4fcd54badfd0c3cee7a6fd8491b94	no	6
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30683 a4fd31454d6499d022aa0f8d84210f32aa7ad0a0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	494646		

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/31 (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.

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Docket Number (Optional): 11913-US-CNT3 4214-25714

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" [37 CFR 1.8(a)]
on _____

Signature _____

Typed or printed name _____

In re Application of: BlackBerry Limited

Application Number	Filed
14/715,227	May 18, 2015

For: System and Method of Owner Application Control of Electronic Devices

Art Unit	Examiner
2876	Daniel A. Hess

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 800.00

☐ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: $ _____

☐ A check in the amount of the fee is enclosed.

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

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☐ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. _____ .

☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is 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.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☑ attorney or agent of record.
Registration number 45,438.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34. _____

/J. Robert Brown, Jr./
Signature

J. Robert Brown, Jr.
Typed or printed name

972-731-2288
Telephone number

February 10, 2016
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 41.31. 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, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14715227
Filing Date:	18-May-2015
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	J. Robert Brown/Judy Fan
Attorney Docket Number:	11913-US-CNT3 4214-25714

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Notice of Appeal	1401	1	800	800
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**800**

Doc Code: AP.PRE.REQ

PTO/SB/33 (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.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
11913-US-CNT3 4214-25714

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 AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed name _____

Application Number	Filed
14/715,227	May 18, 2015

First Named Inventor: Neil P. Adams

Art Unit	Examiner
2876	Daniel A. Hess

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☑ attorney or agent of record.
Registration number 45,438.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/J. Robert Brown, Jr./
Signature

J. Robert Brown, Jr.
Typed or printed name

972-731-2288
Telephone number

February 10, 2016
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

This collection of information is required by 35 U.S.C. 132. 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, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, 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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	BlackBerry Limited	§	
		§	Group Art Unit: 2876
Application No.:	14/715,227	§	
		§	Examiner: Daniel A. Hess
Filed:	May 18, 2015	§	
		§	Confirmation No.: 5874
For:	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES	§	

PRE-APPEAL CONFERENCE BRIEF

In the Office Action mailed November 10, 2015, the Examiner rejected claims 1-5, 9, 10, 12-16, and 20 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication No. 2003/0101292 to Fisher ("Fisher"). Office Action, p. 4. The Examiner also rejected claims 6-8, 11, and 17-19 under 35 U.S.C. 103(a) as being unpatentable over Fisher. Office Action, p. 7.

I. *Fisher does not disclose determining whether the application is allowed to access the local memory based upon an authorization record and an application identifier associated with the application, wherein the authorization record and the application identifier are included in owner control information stored on the electronic device for each application allowed to be executed on the electronic device, and wherein insertion of additional owner control information onto the electronic device is restricted.*

Claim 1 recites "determining whether the application is allowed to access the local memory based upon an authorization record and an application identifier associated with the application, wherein the authorization record and the application identifier are included in owner control information … for each application allowed to be executed on the electronic device." The Office Action asserts Fisher for this element of claim 1 recited above. Office Action, p. 5. Fisher discloses the idea of "sandboxing" whereby "various memory addresses are assigned to one user application and various other memory

addresses are assigned to another [user application] to avoid overlap" and "interference between applications." Fisher, ¶ 4. However, Fisher does not contemplate that such sandboxing is performed in accordance with owner control information that includes **an authorization record and an application identifier for each application allowed to be executed on the electronic device**, as claimed (emphasis added). Unlike claim 1, Fisher is silent regarding any details on how the sandboxing is performed with regard to the applications.

> Next, the Office Action alleges:
>
> "Insertion of additional owner information" would be restricted at least in the sense that another user on the same level could not on their own obtain access to memory and applications belonging to a different user. That is the meaning of assigning users control.

Office Action, p. 6. As quoted above, the Office Action alleges that the claimed "insertion of additional owner control information" is the same as restricting access to memory and applications belonging to a different user. *Office Action*, p. 3. While Fisher discloses sandboxing memory among users and applications, it is not apparent how the ability to sandbox memory has any bearing with respect to restricting the **insertion of additional owner control information onto the electronic device**, as claimed (emphasis added). In fact, Fisher does not contemplate any scenario in which "insertion of additional owner control information onto the electronic device is restricted."

In addition, under "Response to Amendments and Arguments," the Office Action further alleges:

> The examiner draws attention particularly to the 84 page prior art document already of record entitled "Managing Authorization and Access Control" (Windows XP Guide, Published: November 03, 2005 and made of record in the 6/4/2015 IDS, and which this examiner first brought to the attention of the applicants in an earlier application) which shows how access control works in Windows, the world's most common operating system.

Office Action, p. 2. The Examiner appears to be asserting the Windows XP Guide as an additional reference to reject the claims without officially asserting Windows XP Guide under § 102 or § 103. However, the Applicant submits that relying on Windows XP Guide as allegedly teaching the claimed features is improper because **Windows XP Guide does not constitute prior art** with respect to the present application. The present application claims priority to a U.S. provisional application No. 60/432,610 filed on **December 12, 2002**, which predates the publication date of Windows XP Guide, which is November 3, 2005. *See* MPEP § 706.

> The Examiner, under "Response to Amendments and Arguments," also alleges:
>
> The examiner emphasizes that the concept of ownership that Fisher refers to carries with it a tremendous amount of meaning, since the idea of permissions and rights is long established in the realm of operating systems. The examiner has referenced Microsoft Windows because it is the market-dominant operating system running on billions of computers worldwide, but the concepts in the document above are broadly common across operating systems, and predate windows.

Office Action, p. 4. As shown above, the Office Action makes a blanket allegation that the concepts in Windows XP Guide predate windows. First, the Applicant submits that the record is devoid of **factual** evidence that the information relied upon by the Examiner reflects "what a person of ordinary skill in the pertinent art would have known **at the time of the invention**." § MPEP 2141(II). There is no evidence that the claim elements were commonly known **more than thirteen years ago** when the priority application was filed.[1] As technology has widely advanced at rapid rates[2] over the past decade, it cannot be

[1] The present application is a continuation of U.S. Appl. No. 13/618,311, filed on Sep. 14, 2012, now Pat. No. 9,033,216, which is a continuation of U.S. Appl. No. 12/885,281, filed on Sep. 17, 2010, now Pat. No. 8,887,988, which is a continuation of U.S. Appl. No. 11/118,844, filed on Apr. 29, 2005, now Pat. No. 7,815,100, continuation-part of U.S. Appl. No. 13/606,814, filed on Sep. 7, 2012, which is a continuation of U.S. Appl. No. 12/869,589, filed on Aug. 26, 2010, now Pat. No. 8,302,185, which is a continuation of U.S. Appl. No. 10/732,132, filed on Dec. 10, 2003, now Pat. No. 7,793,355, which claims priority to U.S. Appl. 60/432,610, filed on December 12, 2002.

[2] *See* MPEP 2141 ("Factors that may be considered in determining the level of ordinary skill in the art may include…rapidity with which innovations are made").

Nintendo Exhibit 1003
Part 1 of 2
Page 00207

presumed – without avoiding hindsight –that one of ordinary skill in the art would have known *at the time of the invention* that an authorization record and an application identifier are included in owner control information for each application allowed to be executed on an electronic device, wherein the insertion of owner control information is restricted. *See* MPEP § 2141.01 ("The requirement 'at the time the invention was made' is to avoid impermissible hindsight.")

The only evidence to support such a presumption allegedly lies in Windows XP Guide, which, as discussed above, does not constitute prior art. The "legal conclusion must be reached **on the basis of the facts gleaned from the prior art**." MPEP § 2142. Thus, the Examiner "must point to some **concrete evidence** in the record in support of these findings." MPEP § 2144.03(C). "If the examiner is relying on personal knowledge to support the finding of what is known in the art, the examiner must provide an affidavit or declaration setting forth specific factual statements and explanation to support the finding." Since no affidavit or declaration has been provided to support the Examiner's reliance on common knowledge in rejecting the claims, the Applicant respectfully submits that the outstanding claim rejections are not proper and should be withdrawn.

Therefore, claim 1 is not anticipated by Fisher. Claims 12 and 20 recite elements similar to claim 1, and thus, are likewise not anticipated by Fisher. For at least the foregoing reasons, the Applicant respectfully requests the Panel to withdraw the rejections of claims 1, 12, 20, and their dependent claims.

II. *Fisher does not disclose or render obvious that the authorization record is stored in a protected data store, thereby preventing alteration or deletion of the authorization record unless permitted.*

Nintendo Exhibit 1003
Part 1 of 2
Page 00208

Dependent claim 11 recites "wherein the authorization record is stored in a protected data store, thereby preventing alteration or deletion of the authorization record unless permitted." In rejecting this element, the Office Action alleges:

> In the case of organization controlled IT, described above, regular users may not install or delete any application within their allocated space. This an administrative-level function. Users certainly can run applications and operate within applications to create and delete data files associated with those applications, but they may not control the installation and authorizations of applications. This is a protected data store.

Office Action, pp. 7-8. The Examiner asserts the above description based on the Examiner's personal knowledge or opinions as the claimed "protected data store." *Id.* However, this description does not qualify as prior art with respect to the present claims.

Again, the record is devoid of *factual* evidence that the information relied upon by the Examiner reflects "**what a person of ordinary skill in the pertinent art would have known at the time of the invention**." § MPEP 2141(II). Here, the only evidence to support such a presumption lies in the description above, which is based on the Examiner's own understanding or experience, and thus does not constitute prior art. Yet this alone is not sufficient, as "the legal conclusion must be reached on the basis of the **facts gleaned from the prior art**." MPEP § 2142. Thus, the Examiner "must point to some **concrete evidence** in the record in support of these findings."

Respectfully submitted,

CONLEY ROSE, P.C.

Date: February 10, 2016

/J. Robert Brown, Jr./
J. Robert Brown, Jr.
Reg. No. 45,438

ATTORNEY FOR APPLICANTS

5601 Granite Parkway, Suite 500
Plano, Texas 75024
Telephone: (972) 731-2288
Facsimile: (972) 731-2289

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 June 2004 (24.06.2004)

PCT

(10) International Publication Number
WO 2004/053618 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/CA2003/001944

(22) International Filing Date:
12 December 2003 (12.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/432,610 12 December 2002 (12.12.2002) US

(71) Applicant: **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors: **LITTLE, Herbert, A.**; 504 Old Oak Place, Waterloo, Ontario N2T 2V8 (CA). **CLARK, David, R.**; 49 Cedarwoods Cres., Unit 48, Kitchener, Ontario N2C 2L1 (CA).

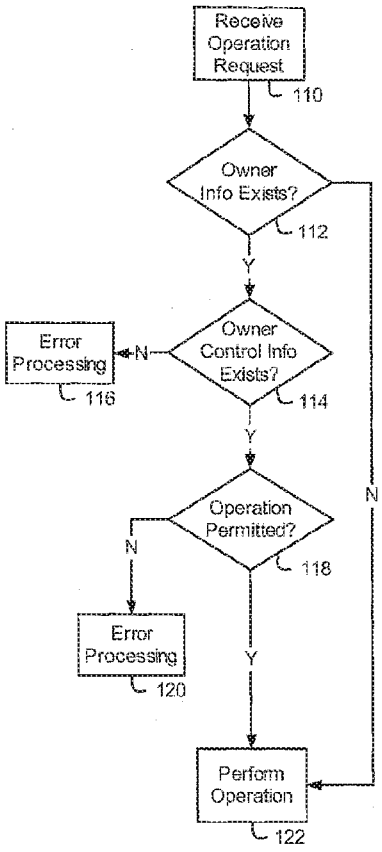
(74) Agents: **WONG, Jeffrey, W.** et al.; Borden Ladner Gervais LLP, 1100-100 Queen Street, Ottawa, Ontario K1P 1J9 (CA).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

[Continued on next page]

(54) Title: SYSTEM AND METHOD OF OWNER CONTROL OF ELECTRONIC DEVICES



(57) Abstract: A system and method of owner control of an electronic device are provided. Owner identification information, such as data integrity and source authentication information, is stored on the electronic device. Received owner control information is stored on the electronic device where the integrity of the received owner control information is verified and/or the source is authenticated using the owner identification information. In one embodiment, owner identification information comprises an owner signature private key.

WO 2004/053618 A2

ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (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.

SYSTEM AND METHOD OF OWNER CONTROL OF ELECTRONIC DEVICES

TECHNICAL FIELD

This system relates generally to electronic devices, and in particular to controlling operations of such devices by a device owner.

BACKGROUND OF THE INVENTION

In a corporate environment, employees are often provided with access to office supplies and equipment to be used in performing job functions. Standard equipment typically includes at least a personal computer (PC), and may also include wireless mobile communication devices and other types of electronic devices. Although such equipment is intended primarily for business or work-related purposes, users sometimes make personal use of office equipment. Employers may be comfortable with some degree of personal use of such equipment, provided that the personal use does not interfere with normal job functions, does not incur additional costs, and conforms with company policies.

In these types of situations, a user of an electronic device is not the owner of the device, and the user and owner may have different perceptions of acceptable device uses. Acceptable uses may be specified in company policies, for example, which employees are expected to follow, but beyond company policy statements, a corporate device owner often has little if any control over how electronic devices are ultimately used. According to one known scheme for controlling operation of electronic devices, an owner loads a policy file onto a device to restrict the type of operations or software applications that may be executed by the device. However, this type of scheme is sometimes circumvented by a user by either deleting the owner policy file or replacing the owner policy file with a user policy file which may include fewer restrictions than the owner policy file. Therefore, there remains a need for a system and method of owner control of electronic devices.

DISCLOSURE OF THE INVENTION

A system of owner control of an electronic device comprises an owner information store configured to store owner information comprising data integrity and/or source authentication information, and an owner control information store configured to store owner control information for controlling operation of the electronic device. The data integrity is used to check the integrity of the received owner control information and/or source authentication information is used to authenticate the source.

Nintendo Exhibit 1003
Part 1 of 2
Page 00212

A method of owner control of electronic devices comprises the steps of storing owner information having data integrity and/or source authentication information on an electronic device, receiving owner control information at the electronic device, and checking integrity of the received owner control information and/or determining whether the authorized source is authentic.

An erase command may be provided to the electronic device, wherein the erase command is digitally signed and indicates that owner information is to be erased from the electronic device. The erase command is performed based upon checking the integrity of the digitally signed erase command.

Further features of owner control systems and methods will be described or will become apparent in the course of the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing a communication system in which electronic devices are used.

Fig. 2 is a block diagram illustrating a system of inserting owner information and owner control information onto an electronic device.

Fig. 3 is a block diagram of an electronic device in which a system and method of owner control are implemented.

Fig. 4 is a flow diagram illustrating a method of inserting owner information onto an electronic device.

Fig. 5 is a flow diagram illustrating a method of inserting owner control information onto an electronic device.

Fig. 6 is a flow diagram showing a method of owner control of an electronic device.

Fig. 7 is a block diagram of a wireless mobile communication device as an example of an electronic device.

BEST MODE FOR CARRYING OUT THE INVENTION

Fig. 1 is a block diagram showing a communication system in which electronic devices are used. The communication system 10 includes a Wide Area Network (WAN) 12, coupled to a computer system 14, a wireless network gateway 16 and a Local Area Network (LAN) 18. The wireless network gateway 16 is also connected to a wireless communication network 20 in which a wireless mobile communication device 22 ("mobile device"), is configured to operate.

Nintendo Exhibit 1003
Part 1 of 2
Page 00213

The computer system 14 is a desktop or laptop PC, which is configured to communicate to the WAN 12, the Internet for example. PCs, such as the computer system 14, normally access the Internet through an Internet Service Provider (ISP), Application Service Provider (ASP) or the like.

The LAN 18 is an example of a typical working environment, in which multiple computers 28 are connected in a network. It is normally located behind a security firewall 24. Within the LAN 18, a message server 26, operating on a computer behind the firewall 24, acts as the primary interface for the corporation to exchange messages both within the LAN 18, and with other external messaging clients via the WAN 12. Known message servers include, for example, Microsoft™ Exchange Server and Lotus Domino™. The LAN 18 includes multiple computer systems 28, each of which implements a messaging client, such as Microsoft Outlook™, Lotus Notes™, Yahoo! ™ Messenger, AOL Instant Messenger, or other client-server or peer-to-peer, or similar messaging clients with various architectures. Messages received by the message server 26 are distributed to mailboxes for user accounts addressed in the received messages, and are then accessed by a user through a messaging client operating on a computer system 28. The fact that the example given illustrates a client-server architecture in no way implies that such architecture is necessary, as other architectures may be used.

Although only a message server 26 is shown in the LAN 18, those skilled in the art will appreciate that a LAN may include other types of servers supporting resources that are shared between the networked computer systems 28, and that the message server 26 may also provide additional functionality, such as dynamic database storage for data such as, but not limited to, calendars, to-do lists, task lists, e-mail and documentation. The message server 26 and electronic messaging are described for illustrative purposes only. Owner control systems and methods are applicable to a wide range of electronic devices, and are in no way limited to electronic devices with messaging capabilities.

The wireless gateway 16 provides an interface to a wireless network 20, through which messages may be exchanged with a mobile device 22. Such functions as addressing of the mobile device 22, encoding or otherwise transforming messages for wireless transmission, and any other interface functions are performed by the wireless gateway 16. The wireless gateway 16 may be configured to operate with more than one wireless network 20, in which case the wireless gateway 16 also determines a most likely network for locating a given mobile device 22 and possibly track mobile devices as users roam between countries or networks.

Nintendo Exhibit 1003
Part 1 of 2
Page 00214

The mobile device 22 is, for example, a data communication device, a voice communication device, a dual-mode communication device such as many modern cellular telephones having both data and voice communications functionality, a multiple-mode device capable of voice, data and other types of communications, a personal digital assistant (PDA) enabled for wireless communications, or a laptop or desktop computer system with a wireless modem.

Any computer system with access to the WAN 12 may exchange messages with the mobile device 22 through the wireless network gateway 16. Alternatively, private wireless network gateways such as wireless Virtual Private Network (VPN) routers could be implemented to provide a private interface to a wireless network. A wireless VPN router implemented in the LAN 18 provides a private interface from the LAN 18 to one or more mobile devices such as 22 through the wireless network 20. A private interface to a mobile device 22 may also effectively be extended to entities outside the LAN 18 by providing a message forwarding or redirection system that operates with the message server 26. Such a message redirection system is disclosed in United States Patent No. 6,219,694, which is hereby incorporated into this application by reference. In this type of system, incoming messages received by the message server 26 and addressed to a user of a mobile device 22 are sent through the wireless network interface, either a wireless VPN router, the wireless gateway 16, or another interface, for example, to the wireless network 20 and to the user's mobile device 22. Another alternate interface to a user's mailbox on a message server 26 may be a Wireless Application Protocol (WAP) gateway. Through a WAP gateway, a list of messages in a user's mailbox on the message server 26, and possibly each message or a portion of each message, may be sent to the mobile device 22.

A wireless network 20 normally delivers messages to and from communication devices such as the mobile device 22 via RF transmissions between base stations and devices. The wireless network 20 may, for example, be a data-centric wireless network, a voice-centric wireless network, or a dual-mode network that can support both voice and data communications over the same infrastructure. Recently developed networks include Code Division Multiple Access (CDMA) networks and General Packet Radio Service (GPRS) networks. So-called third-generation (3G) networks like Enhanced Data rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS) are currently under development. Older data-centric networks include, but are not limited to, the Mobitex™ Radio Network ("Mobitex"), and the DataTAC™ Radio Network ("DataTAC"). Voice-centric data networks such as Personal Communication System (PCS) networks,

Nintendo Exhibit 1003
Part 1 of 2
Page 00215

including Global System for Mobile Communications (GSM) and Time Division Multiple Access (TDMA) systems, have been available in North America and world-wide for several years.

In the system 10, a company that owns the LAN 18 may provide a computer system 28 and a mobile device 22 to an employee. When a computer system 28 issued to an employee is a laptop computer, for example, the computer system 28 may be used either within or outside the corporate LAN 18. When the computer system is operating within the LAN 18, non-local operations may be restricted by configuring permissions and restrictions for the computer system 28, a network account of the user, or both, in such a way that the permissions and restrictions are not configurable by the user. However, if a user is using a computer outside the LAN 18, by connecting the computer to the WAN 12 as shown at 14, for example, network-based controls in place at the LAN 18 can sometimes be bypassed.

In order to maintain control over an electronic device such as the computer system 28 or mobile device 22, an owner may establish local settings directly on the device. Such local settings control device operations, but only as long as the settings remain intact on the device. A common problem with this type of control mechanism is that local settings may be deleted, replaced, or otherwise altered by a user.

Fig. 2 is a block diagram illustrating a system of inserting owner information and owner control information onto an electronic device. The system in Fig. 2 includes an electronic device 210, an owner information insertion point 220, and an owner control information insertion point 230. The owner information insertion point 220 is alternatively referred to as a branding point, while the owner control insertion point 230 is alternatively referred to as a control point. An owner information store 212, an owner control information store 214, and an interface/connector 216 are provided in the electronic device 210. The owner information insertion point 220 includes an owner information source 224 and an interface/connector 222. The owner control information insertion point 230 similarly includes an owner control information source 234 and an interface/connector 232.

The owner information store 212 stores information, such as an owner name or other identification information, for example, which identifies an owner of the electronic device 210. The owner control information store 214 stores information that is used to control the operation of the electronic device 210. Owner control information may, for example, be specified in an authorization record that lists software applications authorized to be installed and executed on the electronic device 210. The use of owner control information to control operations of an electronic device is described in further detail below. The owner information

Nintendo Exhibit 1003
Part 1 of 2
Page 00216

source 224 and the owner control information source 234, could be local memory devices, communication modules through which remote memory devices storing owner information and owner control information are accessible, or possibly user interfaces through which owner information and owner control information are entered.

The interface/connector 222 is compatible with the interface/connector 216 to establish a communication link between the owner information insertion point 220 and the electronic device 210, to thereby enable owner information to be transferred to the electronic device 210 from the owner information source 224. The interface/connector 232 similarly enables transfer of owner control information from the owner control information source 234 onto the electronic device 210 via a communication link established between the interface/connectors 232 and 216. The interface/connectors 216, 222, and 232 may establish wired communication links, where the interface/connectors are serial ports, for example, or wireless communication links such as infrared links where the interface/connectors are infrared modules. Owner information and owner control information transferred to a device are respectively inserted or stored in the owner information store 212 and the owner control information store 214.

The owner control insertion point 220 is associated with an owner of the electronic device 210. Where the electronic device 210 is provided to a user by an employer, for example, the owner control insertion point 220 may be a computer system or device controlled by a corporate computer system administrator or IT department. The electronic device 210 is "branded" with owner information by establishing a communication link between the owner information insertion point 220 and the electronic device 210 through the interface/connectors 222 and 216 and then inserting owner information into the owner information store 212. Unless otherwise desired, once owner information has been inserted onto the mobile device 210, then preferably only the owner or a party authorized by the owner is able to change the owner information or insert or change owner control information on the electronic device 210.

Because insertion of owner control information onto the electronic device 210 is restricted once owner information has been inserted, the owner control information insertion point 230 need not necessarily be controlled by the owner of the electronic device 210. When the owner maintains control over the owner control information insertion point 230, the insertion points 220 and 230 may be implemented in the same computer system or device and share the same interface/connector. However, separate insertion points 220 and 230 as shown in Fig. 2 allow an owner of the electronic device to delegate owner control information

Nintendo Exhibit 1003
Part 1 of 2
Page 00217

insertion to a trusted entity. If owner control information insertion is controlled using digital signatures, for example, as described in further detail below, an owner first brands the electronic device 210 and provides the electronic device 210 and digitally signed owner control information to a user. In this case, the owner control information insertion point 230 may be the user's computer system, which is then used to insert the digitally signed owner control information onto the electronic device 210.

In most implementations, the owner information insertion point 220 and the owner control information control point 230 include the same type of interface/connectors 222 and 232, compatible with the interface/connector 216 in the electronic device 210. However, the electronic device 210 may alternatively include multiple interface/connectors, such that different types of interface/connectors may be implemented at an owner information insertion point 220 and an owner control information insertion point 230. Although only a single owner control information insertion point 220 and owner control information insertion point 230 are shown in Fig. 2, a complete insertion system may include more than one of each type of insertion point. In a large company, for example, corporate computer system administrators may be authorized to perform owner information insertion operations from administrator computer systems, or from any corporate computer system from which administrative functions can be accessed, thereby providing multiple owner information insertion points 220. Similarly, when an owner allows users to insert digitally signed owner control information onto electronic devices, as described above, each user's computer system may be used as an owner control information insertion point 230.

Fig. 3 is a block diagram of an electronic device in which a system and method of owner control are implemented. In Fig. 3, the electronic device is a mobile device 30 adapted to operate within a wireless network. Also shown in Fig. 3 is an insertion tool 64 used to insert owner information onto the mobile device 30.

It should be apparent to those skilled in the art that only the components involved in an owner control system are shown in Fig. 3. A mobile device typically includes further components in addition to those shown in Fig. 3. Also, the mobile device 30 is an illustrative example of an electronic device for which an owner may wish to enforce some sort of usage policy. An owner may also wish to control the usage of other types of electronic devices, such as mobile telephones and PDAs, for example.

As shown in Fig. 3, a mobile device 30 comprises a memory 32, a processor 40, an application loader 42, an insertion module 44, a user interface (UI) 46, a wireless transceiver 48, and an interface/connector 50. The memory 32 preferably includes a software

Nintendo Exhibit 1003
Part 1 of 2
Page 00218

applications store 34, an owner information store 36, an authorization record store 38, as well as possibly other data stores associated with other device systems in addition to those shown in Fig. 3.

The memory 32 is a writable store such as a RAM or Flash memory into which other device components may write data. However, write and erase access to the software application store 34, the owner information store 36, and the authorization record store 38 is preferably restricted. For example, a user of the mobile device 30 may be able to retrieve data from the stores 34, 36, and 38, but write and erase operations for these stores are controlled, as described below. The software application store 34 includes software applications that have been installed on the mobile device 30, and may include, for example, an electronic messaging application, a personal information management (PIM) application, games, as well as other applications. The owner information store 36 stores information such as an owner name or other identification, data integrity and source authentication information, such as a digital signature public key associated with a digital signature private key of the owner. Owner control information, in which an owner of the mobile device 30 specifies usage permissions and restrictions for the mobile device 30, is stored in an authorization record in the authorization record store 38.

The processor 40 is connected to the wireless transceiver 48 and thus enables the mobile device 30 for communications via a wireless network. The application loader 42 and insertion module 44, described in further detail below, are connected to the interface/connector 50 to allow communication with the insertion tool 64, through the co-operating interface/connector 52.

The UI 46 includes one or more UI components, such as a keyboard or keypad, a display, or other components which accept inputs from or provide outputs to a user of the mobile device 30. Although shown as a single block in Fig. 3, it should be apparent that a mobile device 30 typically includes more than one UI, and the UI 46 is therefore intended to represent one or more user interfaces.

The insertion tool 64 includes an owner information store 60 and an interface/connector 52 through which information is exchanged with the mobile device 30, and thus represents an owner information insertion point 220 (Fig. 2). As described above, an owner information insertion point such as the insertion tool 64 is normally controlled by an owner of an electronic device. Therefore, the insertion tool 64 is, for example, implemented on an administrator computer system used by an authorized administrator to enable services for or otherwise configure the mobile device 30. Because networked computer systems can

Nintendo Exhibit 1003
Part 1 of 2
Page 00219

typically be used by any user, the insertion tool 64 may instead be accessible to any computer system in a corporate network, dependent upon the particular user that is currently "logged on" the computer system.

The owner information store 60 stores owner information to be inserted onto the mobile device 30, and may be implemented, for example, on a local memory component such as a RAM chip, a flash memory device, or a hard disk drive. When the insertion tool 64 is implemented in a networked computer system or other network-connected device, the owner information store 60 may be a remote memory system such as a file server that is accessible to the insertion tool 64 through a network connection. The owner information store 60 may instead incorporate a memory reader such as a smart card reader, a memory card reader, a floppy disk drive, or a CD or DVD drive, for example.

Information is transferred between the insertion tool 64 and the mobile device 30 via a communication link established between the interface/connectors 50 and 52. The interface/connectors 50 and 52 could be any of a plurality of compatible data transfer components, including, for example, optical data transfer interfaces such as Infrared Data Association (IrDA) ports, other short-range wireless communications interfaces, or wired interfaces such as serial or Universal Serial Bus (USB) ports and connections. Known short-range wireless communications interfaces include, for example, "Bluetooth" modules and 802.11 modules according to the Bluetooth or 802.11 specifications, respectively. It will be apparent to those skilled in the art that Bluetooth and 802.11 denote sets of specifications, available from the Institute of Electrical and Electronics Engineers (IEEE), relating to wireless LANs and wireless personal area networks, respectively. Therefore, a communication link between the insertion tool 64 and the mobile device 30 may be a wireless connection or a physical wired connection.

Because communications between the insertion tool 64 and the mobile device 30 need not necessarily be accomplished using a physical connection, references to connecting a mobile device to an insertion tool include establishing communications through either physical connections or wireless transfer schemes. Thus, the mobile device 30 could be connected to the insertion tool 64 by connecting serial ports on the mobile device 30 and the insertion tool 64, by positioning the mobile device 30 such that an optical port thereof is in a line of sight of a similar port of the insertion tool 64, or by connecting or arranging the mobile device 30 and the insertion tool 64 in some other manner so that data may be exchanged. The particular operations involved in establishing communications between a mobile device and an insertion tool are dependent upon the types of interfaces and/or connectors available

Nintendo Exhibit 1003
Part 1 of 2
Page 00220

in both the mobile device and the insertion tool.

Owner branding of the mobile device 30 may be facilitated by inserting owner information onto the mobile device 30 using the insertion tool 64 before the mobile device 30 is operable by a user. This may be accomplished, for example, by pre-loading owner information before the mobile device 30 is provided to the user by the owner, or before the mobile device 30 is configured for use. In the former example, the owner maintains physical control of the mobile device 30 until owner information has been loaded, whereas in the latter example, the user has possession of the mobile device 30 but preferably is unable to make use of the device until it is configured by, or at least under the control of, the owner.

Pre-loading of owner information onto the mobile device 30 is performed using the insertion tool 64. As described briefly above, the insertion tool 64 may be a computer system associated with an a owner system administrator, or a computer system which may be used by a mobile device user or administrator. Depending upon the owner information pre-loading scheme, the insertion tool 64 is operated by a mobile device user or an administrator.

When the mobile device 30 has been connected to the insertion tool 64, owner information is retrieved from the owner information store 60 and transferred to the mobile device 30 through the interface/connectors 52 and 50, and passed to the insertion module 44 on the mobile device 30, which stores the owner information to the owner information store 36 in the memory 32.

Although the insertion module 44 is shown in Fig. 3 as being connected to the interface/connector 50, this module is normally implemented as a software module or application that is executed by the processor 40. As such, data transfers to and from the interface/connector 50 may actually be accomplished by routing data through the processor 40 to the interface/connector 50. In this case, the processor 40 may be instructed by the insertion tool 64 to start the insertion module 44 before the owner information is transferred to the mobile device 30. Alternatively, the processor 40 may be configured to start the insertion module 44 whenever owner information is received. The insertion tool 64 may similarly be a software module or application that is executed by a processor (not shown) in a computer system or device on which the insertion tool 64 operates.

The owner information that is pre-loaded onto the mobile device 30 may include data integrity and/or source authentication information, such as a cryptographic system like a digital signature public key which corresponds to a digital signature private key used by the owner to digitally sign information before it is transferred to the mobile device 30. Pre-

Nintendo Exhibit 1003
Part 1 of 2
Page 00221

loading of the data integrity and/or source authentication information enables greater security of owner control operations, as described in further detail below in the context of digital signatures. Owner information may also include, for example, a name or other identifier associated with the owner of the mobile device 30.

In an owner control scheme in which digital signatures are used to verify data integrity and authenticate a source of data, when the owner's digital signature public key has been inserted into the owner information store 36 on the mobile device 30, owner control information, which specifies permissions and/or restrictions for the mobile device 30, is inserted onto the mobile device 30. Although an owner information insertion point, insertion tool 64, is shown in Fig. 3, it will be apparent from Fig. 2 and the above description that owner control information is usually inserted onto an electronic device after the device has been branded by inserting owner information onto the device. An owner control information insertion tool (not shown) configured for use with the mobile device 30 is similar to the insertion tool 64, including an owner control information store and an interface/connector compatible with the interface/connector 50. Owner control information is inserted onto the mobile device 30 and stored in the form of an authorization record in the authorization record store 38. In an authorization record, an owner of the mobile device 30 specifies a list of software applications that a user is authorized to install on the mobile device 30, as well as possibly a list of required software applications that must be installed on the mobile device 30.

In order to prevent a user from inserting false owner control information to thereby circumvent owner control, owner control information is preferably digitally signed using the owner's digital signature private key before being transferred to the mobile device 30. The insertion module 44 is preferably configured to verify the digital signature before the owner control information is stored on the mobile device 30. If digital signature verification fails, then the owner control information is not stored on the mobile device 30.

Digital signature schemes generally involve some sort of transformation of digitally signed information to provide for checking the integrity of the information and authentication of a source of the signed information. For example, according to one known digital signature technique, a digest of information to be digitally signed is first generated using a non-reversible digest algorithm or transformation. Known digest algorithms include Secure Hashing Algorithm 1 (SHA-1) and Message-Digest algorithm 5 (MD5). Other digest techniques that produce a unique digest for each unique input may also be used. The digest is then further transformed using a digital signature private key and a signature algorithm to

Nintendo Exhibit 1003
Part 1 of 2
Page 00222

generate a digital signature. In digital signature verification, a digital signature public key corresponding to the private key is used.

In the context of owner control and owner control information, insertion of the owner's digital signature public key on a mobile device 30 as part of the owner information provides for digital signature-based security of owner control information. If all owner control information is digitally signed before transfer to the mobile device 30, then the insertion module 44 can verify that owner control information has actually been signed using the owner's digital signature private key, known only to the owner, and that the owner control information has not been changed since it was signed. In this manner, only owner control information that originates with the owner of a mobile device 30 is stored to and used on the mobile device 30.

Owner control information is obtained by an owner control information insertion tool from an owner control information store, which may be a remote data store accessible to the insertion tool, a local store, or some form of memory reader, as described above. Owner control information is established based on a set of software applications or functions that the owner wishes to authorize on an electronic device, and usually tends to change relatively infrequently once established. Such owner control information could then be digitally signed by a secure computer system or software component to which only administrators have access, using the owner's digital signature private key. In this case, signed owner control information is then stored at a location that is accessible to administrator computer systems and possibly other computer systems, and retrieved by an owner control information insertion tool as required. The owner control information insertion tool then transfers the signed owner control information to the mobile device 30. Depending upon how often owner control information changes or is expected to change, the signed owner control information may be further distributed to each computer system in a network in order to provide local access to signed owner control information. When new owner control information is generated and signed, the signed new owner control information preferably replaces all existing copies of the owner control information, as described in further detail below. Wide distribution of owner control information provides easier access to the owner control information, whereas shared remote storage of owner control information requires fewer updates when new owner control information is established.

It is also possible to support digital signature generation for owner control information on an owner control information insertion tool. However, in the present example, this would require that the owner control information insertion tool has access to the owner's digital

Nintendo Exhibit 1003
Part 1 of 2
Page 00223

signature private key. Unless otherwise desired, digital signing of owner control information only by secure computer systems or components is generally preferred in that it limits the number of computer systems that can access the owner's digital signature private key.

When signed owner control information is transferred to the insertion module 44, digital signature verification operations are performed. If the digital signature is verified, then the owner control information is stored on the mobile device 30 in the authorization record store 38. Otherwise, the owner control information is not stored. In the event of a digital signature verification failure, an error or like indication may be output to a user on a UI 46 such as a display, an error message may be returned to the owner control information insertion tool, and an indication of the failure may also be output to a user of the owner control information insertion tool. When owner control information insertion fails, retry or other error processing operations may be performed on the owner control information insertion tool, the mobile device 30, or both.

Given the importance of the owner digital signature public key in the present example, at least a first owner information insertion operation for any mobile device 30 is preferably either performed or at least authorized by an administrator, in order to ensure that accurate owner control information is inserted onto the mobile device 30. This prevents a user from circumventing owner control by inserting a digital signature public key other than the owner's digital signature public key onto the mobile device 30.

When owner control information changes, where an owner wishes to expand or further restrict the use of an electronic device, for example, any existing owner control information preferably should be replaced. As described above, new owner control information is preferably digitally signed, and the signed new owner control information is distributed to one or more locations from which it is retrieved for insertion onto electronic devices.

Any of several mechanisms for subsequent distribution of signed new owner control information to electronic devices are possible. When new owner control information is distributed to each owner control information insertion tool, the insertion tool may be configured to detect receipt of new owner control information, and to transfer the new owner control information to the mobile device 30 the next time the mobile device 30 is connected to the owner control information insertion tool. As described above, an owner control information insertion point 230 (Fig. 2), such as an owner control information insertion tool, may be controlled by a user of an electronic device. Many modern electronic devices are configured to be synchronized with computer systems. In such systems, this type of owner

Nintendo Exhibit 1003
Part 1 of 2
Page 00224

control information distribution may be supported by implementing an owner information control insertion tool in a user's computer system. New owner control information is then transferred to the electronic device the next time the electronic device is synchronized with the computer system.

Alternatively, signed new owner control information may be sent by an owner to all owned mobile devices through a wireless network, via the LAN 18, the WAN 12, and the wireless network gateway 16, as shown in Fig. 1, for example. Such signed owner control information could be sent to the owned mobile devices either directly or through one or more owner control information insertion tools. Although the owner's digital signature public key is preferably initially transferred to a mobile device 30 through the interface/connectors 52 and 50, other communication links which cannot be physically secured or protected, such as wireless or public communication network links, may be used to subsequently transfer signed owner control information to an electronic device that is enabled for communications over such other links. When the owner's digital signature public key has been inserted on a mobile device 30, the insertion module 44 is able to verify both the integrity and the source identity of any signed owner control information received, whether it is received via the interface/connector 50 or the wireless transceiver 48. In this type of implementation, for example, an owner control information insertion tool may include a different type of interface to the mobile device 30 than the owner information insertion tool 64.

Initial storage of owner control information, as well as replacement of existing owner control information, is in this example thereby dependent upon verification of a digital signature by the insertion module 44. Those skilled in the art will appreciate that other checks may also be performed before existing information is replaced. In order to prevent replay attacks, in which old owner control information is received by the electronic device, owner control information preferably includes version information. Existing owner control information is replaced only where received owner control information is newer than the existing owner control information. Generally, newer owner control information has a higher version number.

Although owner information is inserted onto the mobile device 30 using the insertion tool 64 as described above, changes to existing owner information, such as when the owner's digital signature private/public key pair is changed, may alternatively be updated on the mobile device 30 using digital signature techniques. To this end, the insertion tool 64 may include other types of communication modules (not shown), such as a wireless transceiver or network connector, for example, that are less secure than the

Nintendo Exhibit 1003
Part 1 of 2
Page 00225

interface/connector 52. In that case, any such updates are dependent upon verification of a digital signature using a digital signature public key in existing owner information.

The foregoing description relates primarily to writing owner information and owner control information to memory on an electronic device such as the mobile device 30. However, an owner may also wish to erase owner information and owner control information, without replacing existing information with new information. In this case, because information is not being written to memory on a device, no signed owner information or owner control information would be sent to the device. Instead, an erase command or request may be sent to the device. Erasure may be a further function supported by the insertion module 44.

Referring again to Fig. 3, if owner information is to be erased from the owner information store 36, then an erase command or request is digitally signed and sent to the insertion module 44. As with new owner information or owner control information, a signed command or request could be sent to the mobile device 30 through either the interface/connector 50 or the wireless transceiver 48. The insertion module 44, using the owner's digital signature public key, executes the command or completes the request only if a digital signature is verified. Otherwise, the command or request may be ignored, and an error or failure indication may be displayed to a user on a UI 46 on the mobile device 30, returned to a sending system or device that sent the command or request, or both. Further error or failure processing routines may then be performed at the sending system or device.

Since owner information includes the owner's digital signature public key in a signature-based owner control scheme, erasure of owner information is preferably tightly controlled. For example, only owner system administrators may be authorized to send erase commands or requests. Sending of signed commands or requests to the mobile device 30 is therefore preferably restricted to administrator computer systems or accounts, an owner information insertion tool, or an owner-controlled erasure tool. For example, an insertion tool such as the insertion tool 64 could be adapted to erase existing owner information from the mobile device 30 by providing an erase command generator or store which is also coupled to the interface/connector 52. Alternatively, owner information erasure could be accomplished using a specialized, owner-controlled erasure tool incorporating such an erase command generator or store and an interface to the mobile device 30. Erasure of owner control information is preferably controlled in a similar manner.

Where an owner control system is configured to support erasure and possibly other owner information and owner control information management functions, access to the

Nintendo Exhibit 1003
Part 1 of 2
Page 00226

owner's digital signature private key is preferably restricted in order to control the information, requests, and commands that can be digitally signed and sent to an electronic device. The digital signature private key or digital signature generation functions may be accessible only to specific computer systems or administrator login accounts, for example.

As shown in Fig. 3, other systems on the mobile device 30 have access to the memory 32. Preferably, no device system should be able to insert, change, or erase owner information or owner control information without submitting properly signed information or commands. Any data stores, such as the owner information store 36 and the authorization record store 38, that store owner information or owner control information are therefore preferably located in protected memory areas. Preferably, only the insertion module 44 has write and erase access to these stores, such that digital signature-based control of insertion and erasure of owner information and owner control information is maintained. Other device systems have read only access to owner information and owner control information. In one possible implementation, any systems or components through which the memory 32 is accessible are configured to allow memory read operations from any locations in the memory 32, but deny any write or erase operations to memory locations storing owner information or owner control information unless the operations originate with or are authorized by the insertion module 44. In an alternative implementation, a memory manager (not shown) is provided to manage all memory access operations. Such a memory manager is configured to direct any write or erase operations involving owner information or owner control information stores to the insertion module 44 for digital signature checking and authorization before completing the operations. Owner information and owner control information may thereby be read by other device systems, but preferably may only be inserted, changed, or erased when a digital signature is verified.

It should be appreciated that the above public key digital signature operations are intended only as an illustrative example. Other digital signature schemes, or other data integrity checking and source authentication schemes, may instead be used to verify the integrity and source of owner control information or commands.

In the mobile device 30, owner control information is included in an authorization record that is stored in the authorization record store 38. An authorization record specifies particular software applications that are authorized for installation on the mobile device 30, and may also specify required software applications that must be installed on the mobile device 30. Such an authorization record provides an electronic device owner with relatively tight control of how a user makes use of the mobile device 30, since only authorized

Nintendo Exhibit 1003
Part 1 of 2
Page 00227

software applications can be loaded onto the device.

Software application loading operations are enabled on the mobile device 30 by the application loader 42. As described above in regard to the insertion module 44, although the application loader 42 is shown as being connected to the interface/connector 50, information may actually be exchanged between the application loader 42 and the interface/connector 50 or the wireless transceiver 48 through the processor 40.

Like owner information and owner control information, software applications may be received by the mobile device 30 via the interface/connector 50 or the wireless transceiver 48. One possible source of software applications configured for operation on the mobile device 30 is a user's computer system equipped with an interface/connector compatible with the interface/connector 50. When the computer system is connected to a corporate LAN, for example, software applications provided by a corporate owner of the mobile device 30 may be retrieved from a file server on the LAN or other store on the LAN, and transferred to the mobile device. A computer system may also or instead obtain software applications for the mobile device 30 from a local store, or other sources, such as Internet-based sources, with which the computer system may communicate.

The application loader 42 is preferably configured to determine whether owner control information is stored on the mobile device 30 whenever a software application is received. If no owner control information is present on the mobile device 30, then no owner controls have been established for the mobile device 30, and the software application is installed. Software application installation typically involves such operations as storing a received application file to the software application store 34 in the memory 32, extracting files for storage to the software application store 34, or possibly executing an installation program or utility. If owner control information is subsequently inserted onto the mobile device 30, existing software applications are preferably checked by either the application loader 42 or the insertion module 44 to ensure that all software applications resident on the mobile device 30 are authorized software applications. Any software applications that have not been authorized are erased from the mobile device 30 or otherwise rendered inoperable.

In some circumstances, owner information may have been inserted onto an electronic device, but owner control information has yet to be inserted. In order to prevent loading of a software application onto the mobile device 30 that subsequently inserted owner control information does not authorize, the mobile device 30 may be substantially disabled, permitting only a limited subset of device functions to be executed, until owner control information is inserted. Alternatively, the application loader 42 may be configured to

Nintendo Exhibit 1003
Part 1 of 2
Page 00228

determine whether owner information is present on the mobile device 30 when a software application is received. Where owner information is found, indicating that owner control information will be established and used for the mobile device 30, the application loader 42 then determines whether owner control information has been inserted. In the event that owner information but not owner control information is found, the application loader 42 does not load the received software application. Error processing operations may then be performed, such as purging the received software application from any temporary memory location in which it was stored when received, and, if memory resources on the mobile device 30 permit, storing the received software application on the mobile device 30 in such a way that it is not executable. Any software applications stored in this manner are then processed by the application loader 42 when owner control information is inserted onto the mobile device 30. Although software applications are stored on the mobile device 30 in this embodiment, they would not be usable until owner control information is inserted onto the mobile device 30, and it is confirmed that the software applications are authorized for installation. The amount of memory space made available for such software applications may occupy is preferably limited, so that available memory space will not be depleted by storing unchecked and possibly unauthorized software applications.

When the application loader 42 determines that owner control information has been inserted onto the mobile device 30, the application loader 42 then determines whether the received software application is authorized for installation on the mobile device 30. If the owner control information includes an authorized software application list, the application loader 42 searches the list to determine whether the received software application is one of the authorized software applications. An authorized software application list preferably includes information that uniquely identifies the authorized software applications, such as a hash of the software application source code or executable code, for example. Because a software application developer is free to choose a file name for any software application, file names may not provide a reliable authorization check. However, if an owner generates a hash of each authorized software application and includes the hash in the owner control information that is inserted onto the mobile device 30, then only particular versions of authorized software applications can be installed on the mobile device 30. The application loader 42 generates a hash of any received software application, and installs the software application only if the generated hash matches a hash in the owner control information. In order to support different hashing algorithms on different electronic devices, a device owner generates more than one hash of each software application and includes each hash in the

Nintendo Exhibit 1003
Part 1 of 2
Page 00229

owner control information inserted onto each owned electronic device. An electronic device may then use any of a number of different hashing algorithms to generate a hash of a received software application. Of course, other unique transformations than hashes could also be used to generate owner control information and to determine whether received software applications are authorized for installation.

Owner control information may also include a required software application list that uniquely identifies software applications that the owner of an electronic device establishes as mandatory. A required software application list allows an owner to ensure that every owned electronic device supports certain core functions, such as electronic messaging and secure communications, for example. Software applications in a required software application list may be uniquely identified by one or more hashes, as described above in the context of authorized applications. The processor 40, application loader 42, insertion module 44, or a further device component or system is configured to periodically check to ensure that each required software application is present on the mobile device 30, and that a hash of each required software application matches a hash in the required software application list. Where a required software application is not present on the device or its hash does not match a hash in the required software application list, which would occur when a software application has been changed, the mobile device 30, or at least some of its functions, is rendered unusable.

In order to provide further control over required software applications, erasure or other operations involving such applications are controlled. Digital signature-based control of such functions is implemented by requiring a digital signature on any erase or write command that affects a required software application. When an erase or write command is received from a system on the mobile device 30 or from a remote system via the interface/connector 50 or wireless transceiver 48, the processor 40 or another device system such as a memory manager (not shown) determines whether the command involves the software application store 34. Such a write or erase command is not executed unless a digital signature is verified using the owner's digital signature public key stored on the mobile device 30. Although software applications may be executed by device systems without requiring digital signatures, required software applications, if so desired, may only be changed or erased when a digital signature is verified. As above, digital signatures represent one possible data integrity and source authentication mechanism.

Fig. 4 is a flow diagram illustrating a method of inserting owner information onto an electronic device. The method in Fig. 4 begins at step 72, when an electronic device owner

Nintendo Exhibit 1003
Part 1 of 2
Page 00230

establishes owner information. This involves such operations as selecting an owner name or identifier and generating or obtaining an owner digital signature private/public key pair, for example. The owner information is then digitally signed and sent to the electronic device at step 74.

At step 76, a determination is made as to whether owner information already exists on the electronic device, by checking an owner information store, for example. When owner information does not exist on the electronic device, such as for an initial insertion of owner information, the owner information is inserted onto the electronic device at step 84, by storing the owner information to a memory on the electronic device. When the owner information is initially being inserted onto the electronic device, it need not necessarily be digitally signed. As described above, initial owner information insertion is preferably performed directly by or at least under the authorization of the owner or an owner system administrator.

A digital signature associated with the owner information is checked at step 78 where owner information already exists on the electronic device. If the digital signature is not verified, as determined at step 80, the owner information cannot be inserted onto the electronic device, and error processing is invoked at step 82. As described above, error processing may include such operations as indicating an error or failure on a UI of the electronic device and sending an error or failure message to an insertion tool or system from which the owner information was sent. The owner information is inserted onto the electronic device at step 84 where the digital signature was verified.

Once owner information has been inserted onto an electronic device, owner control information is inserted onto the electronic device to set up owner controls. Fig. 5 is a flow diagram illustrating a method of inserting owner control information onto an electronic device.

At step 92, owner control information is established, based on how an owner wishes to control an electronic device. Owner control information, as described above, may include an authorized software application list and a required software application list., for example. The owner control information is then signed and sent to the electronic device at step 94. The digital signature on the owner control information is then checked at step 96. At step 98, it is determined whether the digital signature is verified. Error processing, which may involve operations similar to those described above in conjunction with step 82 in Fig. 4, is performed at step 100. If owner information including the owner's digital signature public key has not been previously inserted onto the electronic device, or the owner control information

Nintendo Exhibit 1003
Part 1 of 2
Page 00231

was not signed using the digital signature private key corresponding to the owner digital signature public key inserted onto the electronic device, then the digital signature is not verified at step 98.

When the digital signature is verified at step 98, it is then determined at step 101 whether the received owner control information is current, such as by determining whether a version number of the received owner control information is greater than the version number of existing owner control information. The owner control information is inserted onto the electronic device at step 102 when the digital signature was verified and the received owner control information is current, by storing the information to an appropriate data store on the electronic device, for example. Otherwise, error processing is performed at step 100.

Other operations may also be dependent upon verification of digital signatures. For example, commands or requests to write data to or erase data from an owner information store, an owner control information store, or a software application store may be similarly processed to verify associated digital signatures before the commands or requests are completed.

Owner control information is then used to control the electronic device. Fig. 6 is a flow diagram showing a method of owner control of an electronic device. At step 110, an operation request is received at the electronic device. Operation requests include, for example, receipt of a software application for installation, a function call from a software application executing on the electronic device, an attempt by a user, software application, or a system on the electronic device to perform an operation, and the like. Such requests may originate with a user, a software application, a device system, or possibly a remote system or device. If owner information does not exist on the electronic device, as determined at step 112, then owner controls have not been established and the operation is performed at step 122. In the example of a received software application, step 122 involves installation of the software application on the electronic device.

When owner information exists, it is determined at step 114 whether owner control information exists. Error processing operations are performed at step 116 if owner information, but not owner control information, exists. As described above, determining whether owner information exists at step 112, and then reverting to error processing at step 116 where it is determined at step 114 that owner control information does not exist prevents certain operations, such as software application loading and installation, when an owner information has been inserted onto an electronic device, but owner control information has not yet been inserted. Step 116 may include such operations as presenting an error

Nintendo Exhibit 1003
Part 1 of 2
Page 00232

message to a user of the electronic device and returning an error indication to a source from which the operation request was received. Alternatively, default action in response to a negative determination at step 114 could be to revert to step 122, when an owner does not wish to restrict device operations before owner control information is inserted.

When both owner information and owner control information have been inserted onto an electronic device, it is determined at step 118 whether the operation is permitted. In the case of a received software application, step 118 involves determining whether software application installation is permitted, and possibly whether the software application is an authorized software application. The operation is performed at step 122 where the operation is permitted. Otherwise, error processing is performed at step 120. As described above, owner control information may include not only permissions and restrictions for electronic device operations and software applications, but also a list of required software applications or modules which may be checked from time to time to ensure that all required software applications are present on an electronic device. For example, an electronic device may be configured to check for required software applications at step 118 when certain types of operation request are received, and to perform the operation at step 122 only when all required software applications are found.

It will be appreciated that the above description relates to preferred embodiments by way of example only. Many variations on the systems and methods described above will occur to those knowledgeable in the field, and such variations are within the scope of the invention as described, whether or not expressly described.

For example, owner information and owner control information operations may be secured by other means than digital signatures. Instead of checking digital signatures on owner information, owner control information, and restricted commands or requests, an electronic device might issue a cryptographic challenge using a previously inserted encryption key associated with the owner. The encryption key could be a public key of the owner or a secret key shared between the owner and the electronic device. Operations such as owner information or owner control information insertion or erasure would then be performed only when a valid challenge response is returned. As those skilled in the art will appreciate, a valid challenge response can only be generated using a corresponding encryption key. Data integrity and source authentication could instead be assumed, for example, where owner information and owner control information are sent to an electronic device over a secure channel. If the device properly decrypts information received via the secure channel, then it is assumed that the information is valid and was sent by an

Nintendo Exhibit 1003
Part 1 of 2
Page 00233

authorized source. In this latter scheme, the source and device share a public/private key pair, or a common symmetric key.

In addition, an electronic device in which systems and methods described above are implemented may include fewer, further, or additional components than shown in Figs. 2 and 3. Fig. 7 is a block diagram of a wireless mobile communication device as an example of such an electronic device. However, it should be understood that the systems and methods disclosed herein may be used with many different types of devices, such as personal digital assistants (PDAs) and desktop computers.

The mobile device 500 is preferably a two-way communication device having at least voice and data communication capabilities. The mobile device 500 preferably has the capability to communicate with other computer systems on the Internet. Depending on the functionality provided by the mobile device, the mobile device may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device (with or without telephony capabilities). As mentioned above, such devices are referred to generally herein as mobile devices.

The mobile device 500 includes a transceiver 511, a microprocessor 538, a display 522, non-volatile memory 524, random access memory (RAM) 526, auxiliary input/output (I/O) devices 528, a serial port 530, a keyboard 532, a speaker 534, a microphone 536, a short-range wireless communications sub-system 540, and may also include other device sub-systems 542. The transceiver 511 preferably includes transmit and receive antennas 516, 518, a receiver (Rx) 512, a transmitter (Tx) 514, one or more local oscillators (LOs) 513, and a digital signal processor (DSP) 520. Within the non-volatile memory 524, the mobile device 500 includes a plurality of software modules 524A-524N that can be executed by the microprocessor 538 (and/or the DSP 520), including a voice communication module 524A, a data communication module 524B, and a plurality of other operational modules 524N for carrying out a plurality of other functions.

The mobile device 500 is preferably a two-way communication device having voice and data communication capabilities. Thus, for example, the mobile device 500 may communicate over a voice network, such as any of the analog or digital cellular networks, and may also communicate over a data network. The voice and data networks are depicted in Fig. 7 by the communication tower 519. These voice and data networks may be separate communication networks using separate infrastructure, such as base stations, network controllers, etc., or they may be integrated into a single wireless network. References to the

Nintendo Exhibit 1003
Part 1 of 2
Page 00234

network 519 should therefore be interpreted as encompassing both a single voice and data network and separate networks.

The communication subsystem 511 is used to communicate with the network 519. The DSP 520 is used to send and receive communication signals to and from the transmitter 514 and receiver 512, and also exchange control information with the transmitter 514 and receiver 512. If the voice and data communications occur at a single frequency, or closely-spaced set of frequencies, then a single LO 513 may be used in conjunction with the transmitter 514 and receiver 512. Alternatively, if different frequencies are utilized for voice communications versus data communications or the mobile device 500 is enabled for communications on more than one network 519, then a plurality of LOs 513 can be used to generate frequencies corresponding to those used in the network 519. Although two antennas 516, 518 are depicted in Fig. 7, the mobile device 500 could be used with a single antenna structure. Information, which includes both voice and data information, is communicated to and from the communication module 511 via a link between the DSP 520 and the microprocessor 538.

The detailed design of the communication subsystem 511, such as frequency band, component selection, power level, etc., is dependent upon the communication network 519 in which the mobile device 500 is intended to operate. For example, a mobile device 500 intended to operate in a North American market may include a communication subsystem 511 designed to operate with the Mobitex or DataTAC mobile data communication networks and also designed to operate with any of a variety of voice communication networks, such as AMPS, TDMA, CDMA, PCS, etc., whereas a mobile device 500 intended for use in Europe may be configured to operate with the GPRS data communication network and the GSM voice communication network. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile device 500.

Communication network access requirements for the mobile device 500 also vary depending upon the type of network 519. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each device. In GPRS data networks, however, network access is associated with a subscriber or user of the mobile device 500. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate the mobile device 500 on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM, but the mobile device 500 is unable to carry out functions involving communications over the network 519, other than any legally required

Nintendo Exhibit 1003
Part 1 of 2
Page 00235

operations, such as '911' emergency calling.

After any required network registration or activation procedures have been completed, the mobile device 500 is able to send and receive communication signals, preferably including both voice and data signals, over the network 519. Signals received by the antenna 516 from the communication network 519 are routed to the receiver 512, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding, to be performed using the DSP 520. In a similar manner, signals to be transmitted to the network 519 are processed, including modulation and encoding, for example, by the DSP 520 and are then provided to the transmitter 514 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 519 via the antenna 518. Although a single transceiver 511 is shown for both voice and data communications, in alternative embodiments, the mobile device 500 may include multiple distinct transceivers, such as a first transceiver for transmitting and receiving voice signals, and a second transceiver for transmitting and receiving data signals, or a first transceiver configured to operate within a first frequency band, and a second transceiver configured to operate within a second frequency band.

In addition to processing the communication signals, the DSP 520 also provides for receiver and transmitter control. For example, the gain levels applied to communication signals in the receiver 512 and transmitter 514 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 520. Other transceiver control algorithms could also be implemented in the DSP 520 in order to provide more sophisticated control of the transceiver 511.

The microprocessor 538 preferably manages and controls the overall operation of the mobile device 500. Many types of microprocessors or microcontrollers could be used here, or, alternatively, a single DSP 520 could be used to carry out the functions of the microprocessor 538. Low-level communication functions, including at least data and voice communications, are performed through the DSP 520 in the transceiver 511. High-level communication applications, including the voice communication application 524A, and the data communication application 524B are stored in the non-volatile memory 524 for execution by the microprocessor 538. For example, the voice communication module 524A may provide a high-level user interface operable to transmit and receive voice calls between the mobile device 500 and a plurality of other voice devices via the network 519. Similarly,

Nintendo Exhibit 1003
Part 1 of 2
Page 00236

the data communication module 524B may provide a high-level user interface operable for sending and receiving data, such as e-mail messages, files, organizer information, short text messages, etc., between the mobile device 500 and a plurality of other data devices via the network 519.

The microprocessor 538 also interacts with other device subsystems, such as the display 522, RAM 526, auxiliary I/O devices 528, serial port 530, keyboard 532, speaker 534, microphone 536, a short-range communications subsystem 540 and any other device subsystems generally designated as 542. For example, the modules 524A-N are executed by the microprocessor 538 and may provide a high-level interface between a user of the mobile device and the mobile device. This interface typically includes a graphical component provided through the display 522, and an input/output component provided through the auxiliary I/O devices 528, keyboard 532, speaker 534, or microphone 536. Such interfaces are designated generally as UI 46 in Fig. 3.

Some of the subsystems shown in Fig. 7 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard 532 and display 522 may be used for both communication-related functions, such as entering a text message for transmission over a data communication network, and device-resident functions such as a calculator or task list or other PDA type functions.

Operating system software used by the microprocessor 538 is preferably stored in a persistent store such as the non-volatile memory 524. In addition to the operating system and communication modules 524A-N, the non-volatile memory 524 may include a file system for storing data. The non-volatile memory 524 may also include data stores for owner information and owner control information. The operating system, specific device applications or modules, or parts thereof, may be temporarily loaded into a volatile store, such as RAM 526 for faster operation. Moreover, received communication signals may also be temporarily stored to RAM 526, before permanently writing them to a file system located in the non-volatile memory 524. The non-volatile memory 524 may be implemented, for example, with Flash memory, non-volatile RAM, or battery backed-up RAM.

An exemplary application module 524N that may be loaded onto the mobile device 500 is a PIM application providing PDA functionality, such as calendar events, appointments, and task items. This module 524N may also interact with the voice communication module 524A for managing phone calls, voice mails, etc., and may also interact with the data communication module 524B for managing e-mail communications and other data

Nintendo Exhibit 1003
Part 1 of 2
Page 00237

transmissions. Alternatively, all of the functionality of the voice communication module 524A and the data communication module 524B may be integrated into the PIM module.

The non-volatile memory 524 preferably provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules 524A, 524B, via the wireless network 519. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless network 519, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.

The mobile device 500 is manually synchronized with a host system by placing the mobile device 500 in an interface cradle, which couples the serial port 530 of the mobile device 500 to a serial port of the host system. The serial port 530 may also be used to insert owner information and owner control information onto the mobile device 500 and to download other application modules 524N for installation on the mobile device 500. This wired download path may further be used to load an encryption key onto the mobile device 500 for use in secure communications, which is a more secure method than exchanging encryption information via the wireless network 519.

Owner information, owner control information and additional application modules 524N may be loaded onto the mobile device 500 through the network 519, through an auxiliary I/O subsystem 528, through the short-range communications subsystem 540, or through any other suitable subsystem 542, and installed by a user in the non-volatile memory 524 or RAM 526. Such flexibility in application installation increases the functionality of the mobile device 500 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the mobile device 500.

When the mobile device 500 is operating in a data communication mode, a received signal, such as a text message or a web page download, will be processed by the transceiver 511 and provided to the microprocessor 538, which preferably further processes the received signal for output to the display 522, or, alternatively, to an auxiliary I/O device 528. Owner information, owner control information, commands or requests related to owner information or owner control information, and software applications received by the transceiver 511 are processed as described above. A user of mobile device 500 may also compose data items, such as email messages, using the keyboard 532, which is preferably a

Nintendo Exhibit 1003
Part 1 of 2
Page 00238

complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device 500 is further enhanced with the plurality of auxiliary I/O devices 528, which may include a thumbwheel input device, a touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user are then transmitted over the communication network 519 via the transceiver 511.

When the mobile device 500 is operating in a voice communication mode, the overall operation of the mobile device 500 is substantially similar to the data mode, except that received signals are output to the speaker 534 and voice signals for transmission are generated by a microphone 536. In addition, the secure messaging techniques described above might not necessarily be applied to voice communications. Alternative voice or audio I/O devices, such as a voice message recording subsystem, may also be implemented on the mobile device 500. Although voice or audio signal output is accomplished through the speaker 534, the display 522 may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information. For example, the microprocessor 538, in conjunction with the voice communication module 524A and the operating system software, may detect the caller identification information of an incoming voice call and display it on the display 522.

A short-range communications subsystem 540 is also be included in the mobile device 500. For example, the subsystem 540 may include an infrared device and associated circuits and components, or a Bluetooth or 802.11 short-range wireless communication module to provide for communication with similarly-enabled systems and devices. Thus, owner information insertion, owner control information insertion, and application loading operations as described above may be enabled on the mobile device 500 via the serial port 530 or other short-range communications subsystem 540.

Fig. 7 represents a specific example of an electronic device in which owner control systems and methods described above may be implemented. Implementation of such systems and methods in other electronic devices having further, fewer, or different components than those shown in Fig. 7 would occur to one skilled in the art to which this application pertains and are therefore considered to be within the scope of the present invention. For example, although a SIM card has not been explicitly shown in Fig. 7, it should be appreciated that implementation of owner control systems and methods in electronic devices with SIM cards is contemplated. Since SIM cards currently incorporate a memory component, owner information, owner control information, or both, may be inserted

Nintendo Exhibit 1003
Part 1 of 2
Page 00239

onto a SIM card and used to maintain owner control of an electronic device when the SIM card is installed in the electronic device. In this case, a SIM card could be branded by inserting owner information onto the SIM card, and owner control information could then be inserted onto the SIM card or an electronic device in which the SIM card is installed.

The above-described embodiments of the present invention are intended to be examples only. Alterations, modifications and variations may be effected to the particular embodiments by those of skill in the art without departing from the scope of the invention, which is defined solely by the claims appended hereto.

INDUSTRIAL APPLICABILITY

The present invention is directed at controlling operations of electronic devices.

Nintendo Exhibit 1003
Part 1 of 2
Page 00240

WHAT IS CLAIMED IS:

1. A method of owner control of electronic devices, comprising the steps of:

receiving, at an electronic device, owner information which includes owner identification information;

receiving, at the electronic device, owner control information;

using the received owner identification information to check integrity of the received owner control information; and

determining whether to use the received owner control information on the electronic device based upon the check of the integrity of the owner control information.

2. The method of claim 1, wherein the owner identification information includes data integrity information which is used to check the integrity of the received owner control information.

3. The method of claim 2, wherein the data integrity information of the owner information is a digital signature.

4. The method of claim 1, wherein the owner identification information includes source authentication information which is used to authenticate source of the owner control information.

5. The method of claim 4, determining whether to use the received owner control information based upon the source of the owner control information being authenticated.

6. The method of claim 5, wherein the source is an authorized source.

7. The method of claim 6, wherein the authorized source is owner of the electronic device.

8. The method of claim 6, wherein the authorized source is a source acting on behalf of the owner.

9. The method of claim 1, further comprising the step of checking integrity of the owner

Nintendo Exhibit 1003
Part 1 of 2
Page 00241

identification information by use of a digital signature.

10. The method of claim 9, wherein the digital signature is created by application of a cryptographic algorithm to the owner information.

11. The method of claim 10, wherein the cryptographic algorithm includes use of a symmetric key.

12. The method of claim 10, wherein the cryptographic algorithm includes use of a asymmetric key.

13. The method of claim 1, wherein the owner control information comprises a description of functions or software applications the electronic device is allowed to use.

14. The method of claim 1, wherein the owner control information comprises a description of functions or software applications the electronic device is prohibited to use.

15. The method of claim 1, wherein the owner control information comprises a description of functions or software applications the electronic device is permitted to use in a modified manner.

16. The method of claim 1, further comprising the step of determining whether to perform an operation on the electronic device based upon whether the owner information exists on the electronic device.

17. The method of claim 1, further comprising the step of determining whether to perform an operation on the electronic device based upon whether the owner control information exists on the electronic device.

18. The method of claim 1, further comprising the step of determining whether to perform an operation on the electronic device based upon an operation permissions list contained in the owner control information.

19. The method of claim 1, further comprising the steps of:

Nintendo Exhibit 1003
Part 1 of 2
Page 00242

receiving, at the electronic device, an erase command;

wherein the erase command indicates that the owner information is to be erased from the electronic device;

wherein the erase command is digitally signed;

determining whether to perform the erase command based upon checking integrity of the digitally signed erase command.

20. The method of claim 1, wherein the owner control information includes an authorized software application list;

wherein the authorized software application list identifies an authorized software application by a hash of the software application;

wherein the software application is used on the electronic device based upon an integrity check using the hash of the software application.

21. The method of claim 1, wherein the electronic device is a wireless mobile communications device.

22. The method of claim 1, wherein the electronic device is a desktop computer.

23. The method of claim 1, wherein the electronic device is a personal digital assistant (PDA).

24. The method of claim 1, further comprising the steps of:

issuing a cryptographic challenge using an encryption key stored on the electronic device and which is associated with owner of the electronic device;

determining whether to perform an operation on the electronic device based upon determination of the issued cryptographic challenge.

25. The method of claim 24, wherein the encryption key is a public key of the owner or a secret key shared between the owner and the electronic device.

26. A data signal that is transmitted using a communication channel, wherein the data signal includes the owner information of claim 1.

Nintendo Exhibit 1003
Part 1 of 2
Page 00243

27. Computer-readable medium capable of causing an electronic device to perform the method of claim 1.

28. A system for owner control of an electronic device, comprising:

an owner information store configured to store owner information having data integrity information;

an owner control information store configured to store owner control information for controlling operation of an electronic device;

wherein the stored data integrity information is used to check integrity of the owner control information;

wherein whether to use the received owner control information on the electronic device is determined based upon the check of the integrity of the owner control information.

29. The system of claim 28 further comprising an insertion module configured to receive owner control information.

30. An apparatus of owner control of electronic devices, comprising:

means for receiving, at an electronic device, owner information which includes owner identification information;

means for receiving, at the electronic device, owner control information;

means for using the received owner identification information to check integrity of the received owner control information; and

means for determining whether to use the received owner control information on the electronic device based upon the check of the integrity of the owner control information.

Nintendo Exhibit 1003
Part 1 of 2
Page 00244

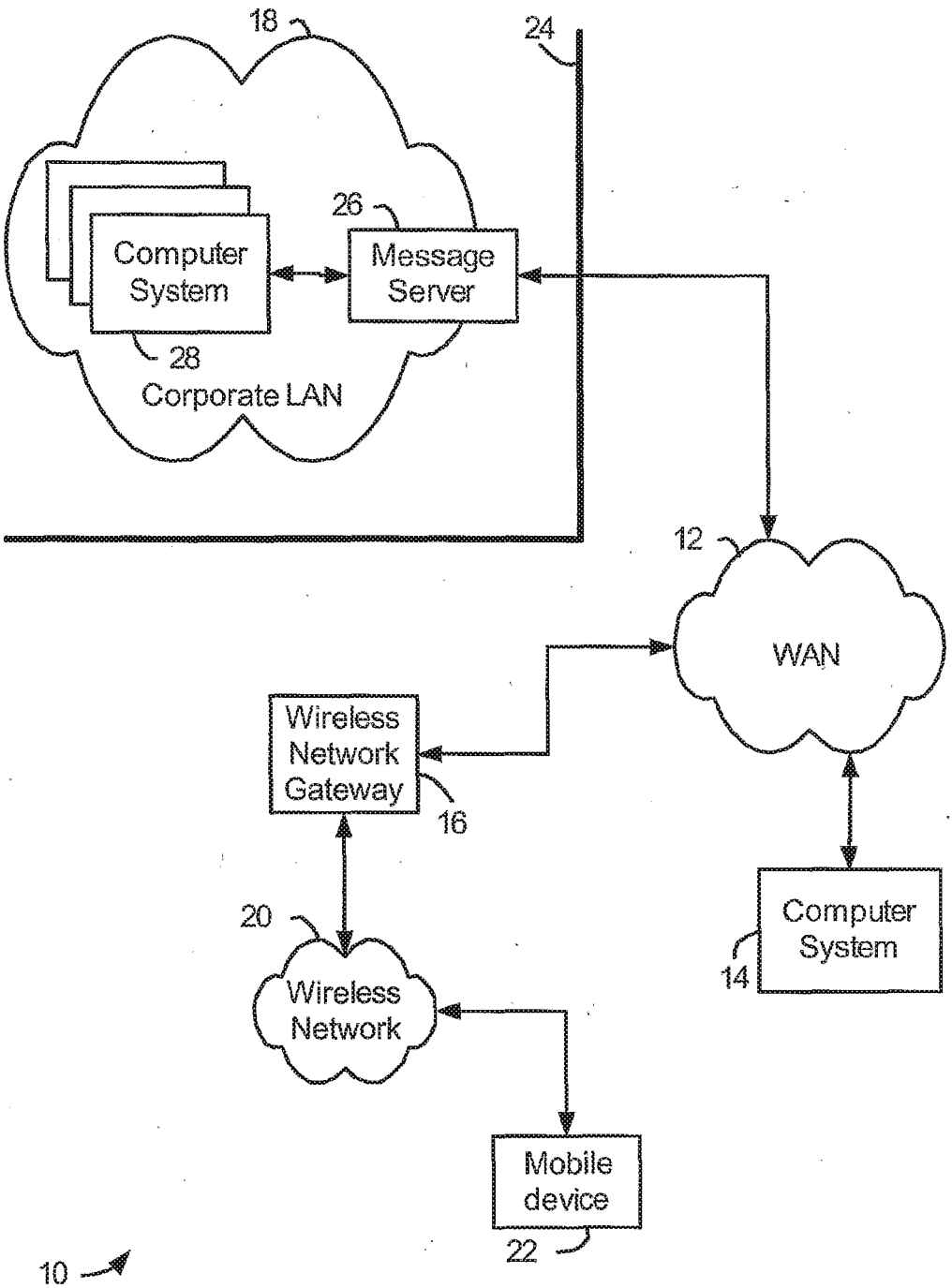

18
24
26
Computer System
Message Server
28
Corporate LAN
12
WAN
Wireless Network Gateway
16
20
Wireless Network
Computer System
14
Mobile device
22
10

FIG. 1

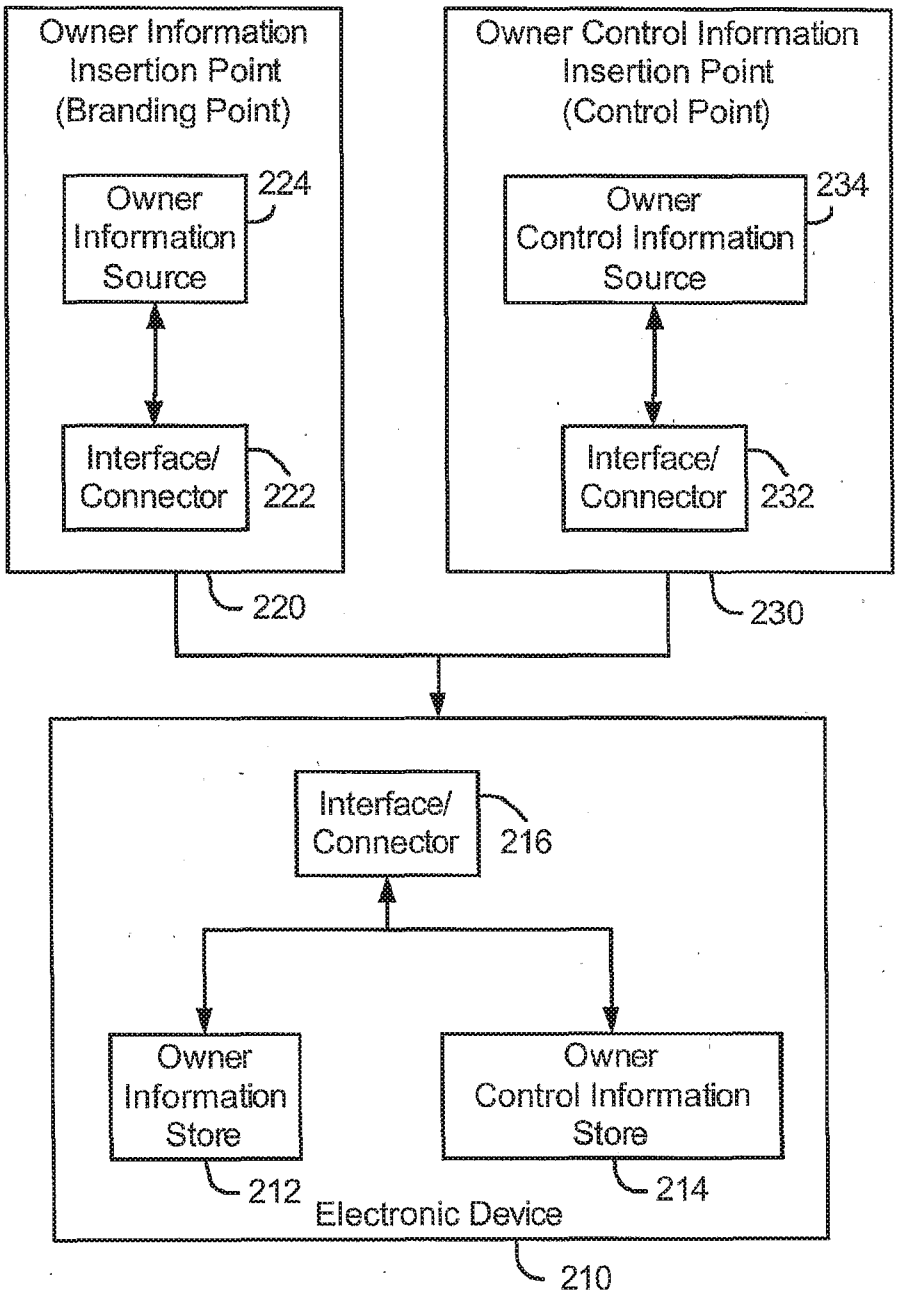

Owner Information Insertion Point (Branding Point)
Owner Information Source
224
Interface/ Connector
222
220
Owner Control Information Insertion Point (Control Point)
Owner Control Information Source
234
Interface/ Connector
232
230
Interface/ Connector
216
Owner Information Store
212
Owner Control Information Store
214
Electronic Device
210

FIG. 2

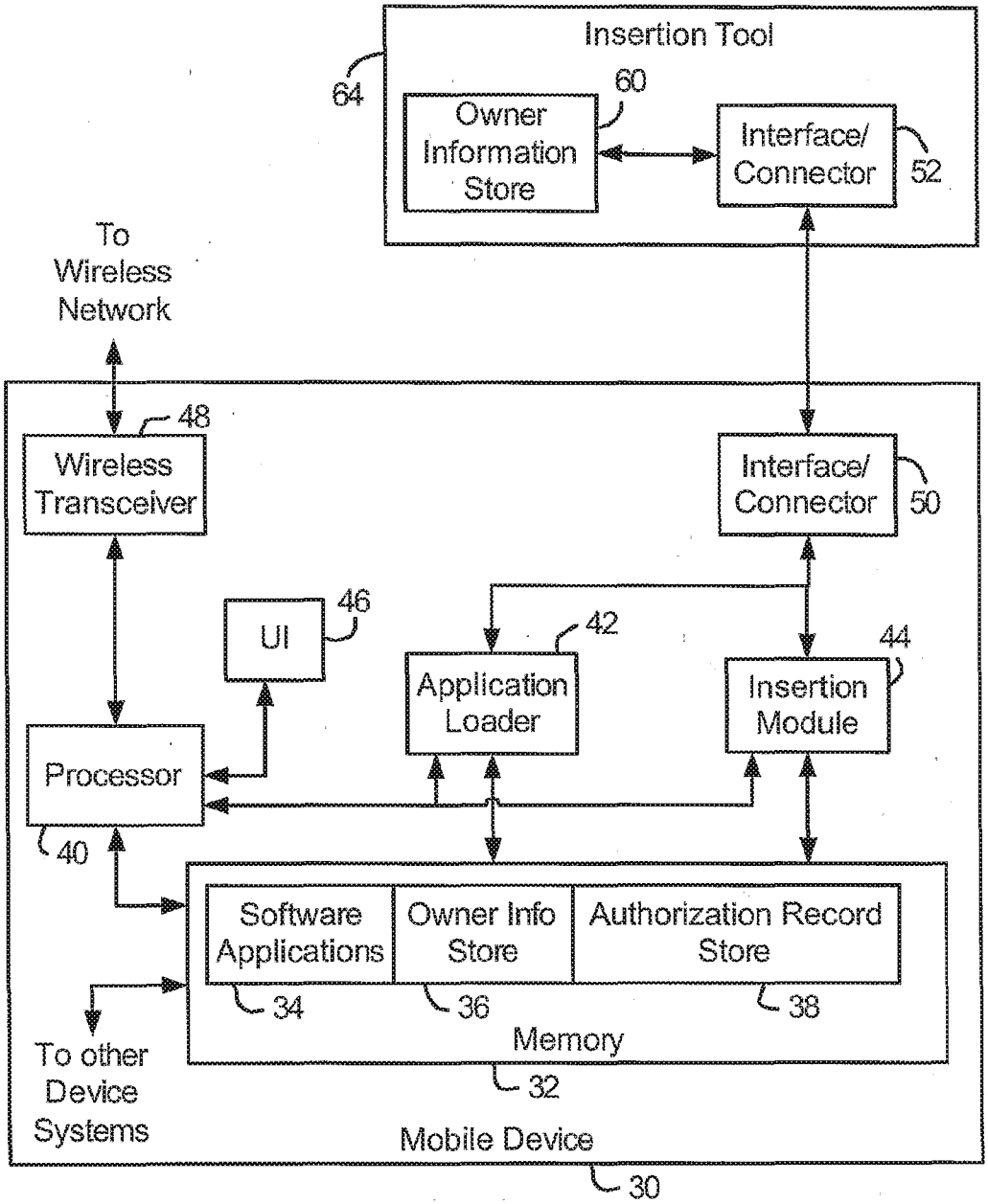

Insertion Tool
64
60
Owner Information Store
Interface/ Connector
52
To Wireless Network
48
Wireless Transceiver
Interface/ Connector
50
UI
46
42
Application Loader
44
Insertion Module
Processor
40
Software Applications
Owner Info Store
Authorization Record Store
34
36
38
Memory
32
To other Device Systems
Mobile Device
30

FIG. 3

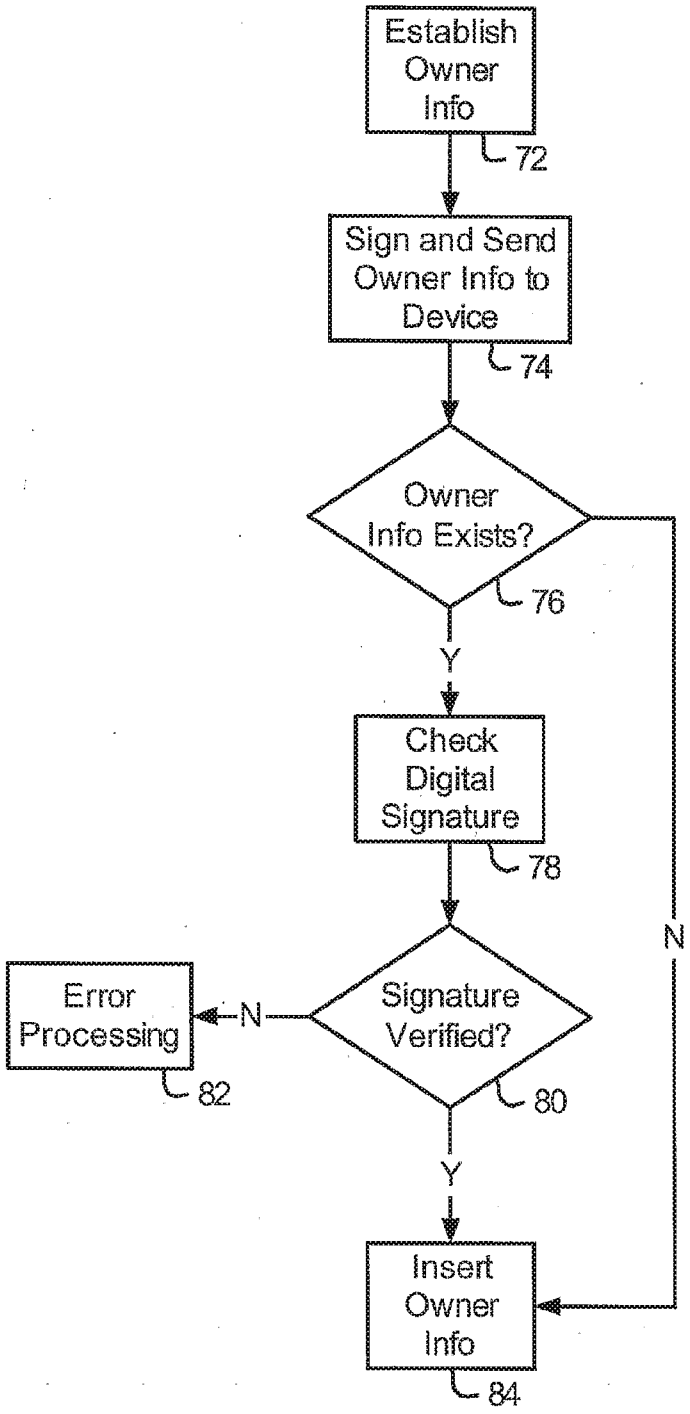

Establish Owner Info
72
Sign and Send Owner Info to Device
74
Owner Info Exists?
76
Y
N
Check Digital Signature
78
Signature Verified?
80
N
Error Processing
82
Y
Insert Owner Info
84

FIG. 4

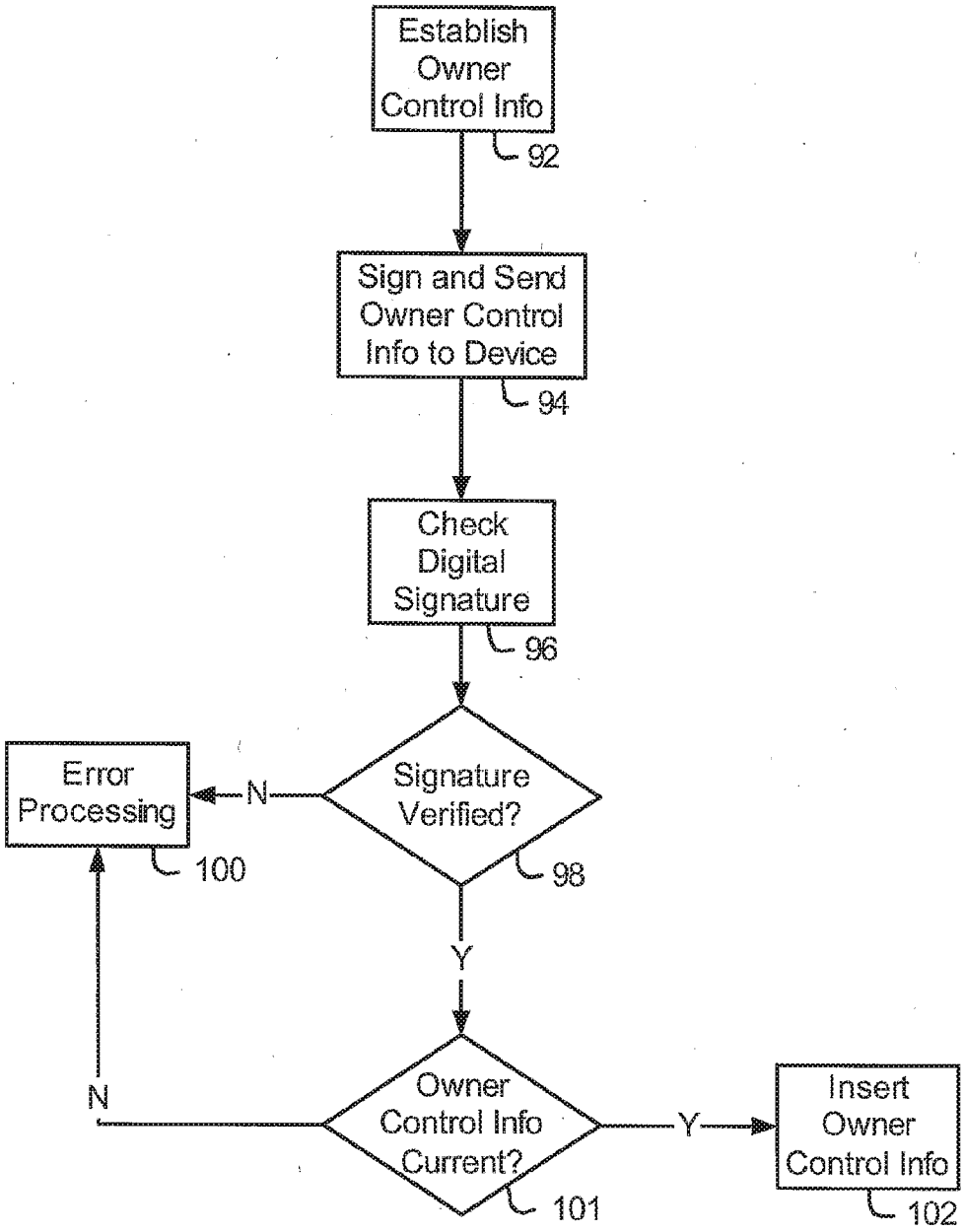

Establish Owner Control Info
92
Sign and Send Owner Control Info to Device
94
Check Digital Signature
96
Signature Verified?
98
N
Error Processing
100
Y
Owner Control Info Current?
101
N
Y
Insert Owner Control Info
102

FIG. 5

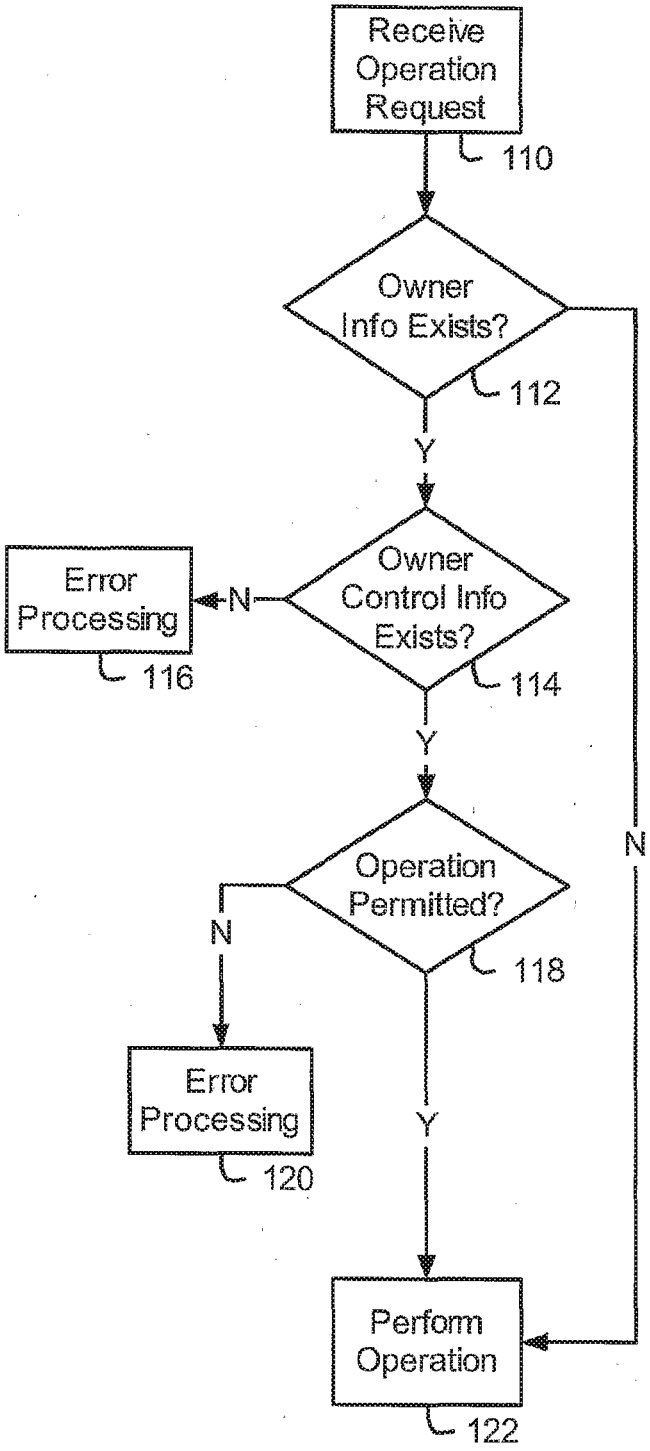

Receive Operation Request
110
Owner Info Exists?
112
Y
N
Owner Control Info Exists?
114
N
Error Processing
116
Y
Operation Permitted?
118
N
Error Processing
120
Y
Perform Operation
122

FIG. 6

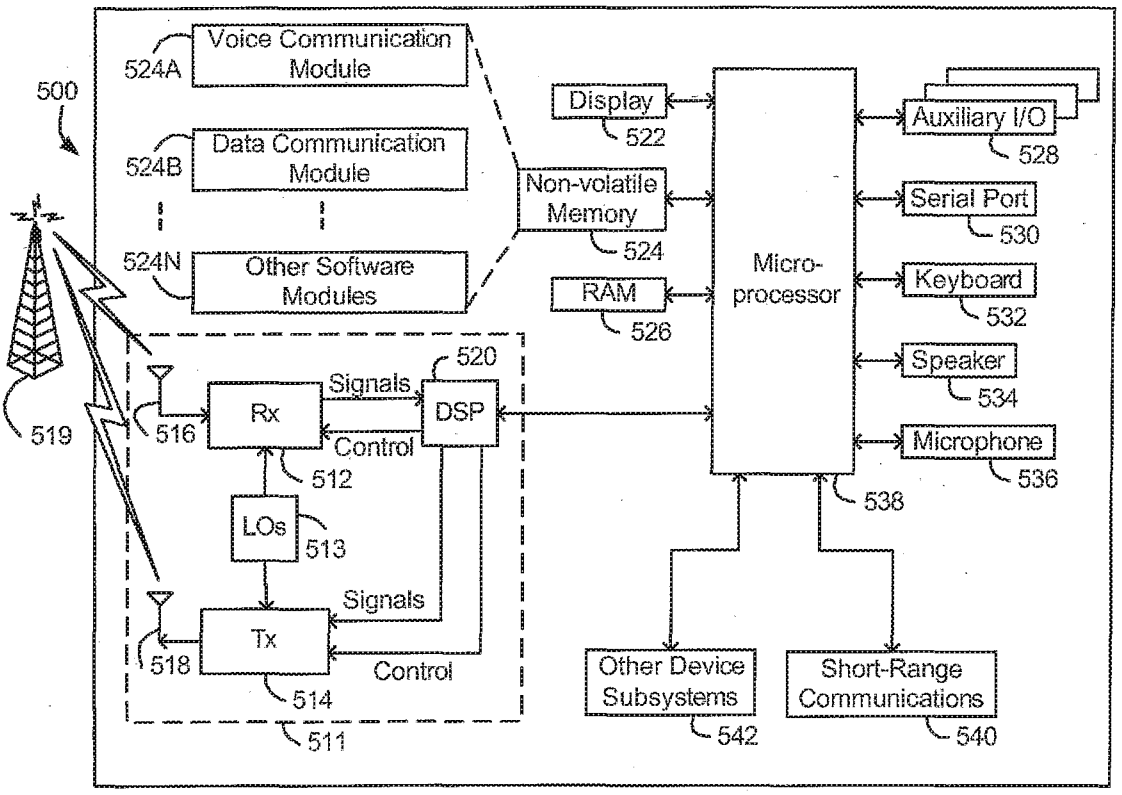


FIG. 7

Nintendo Exhibit 1003
Part 1 of 2
Page 00251

Electronic Acknowledgement Receipt

EFS ID:	24712315
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Rami Law
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	25-JAN-2016
Filing Date:	18-MAY-2015
Time Stamp:	14:39:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	507
Deposit Account	501515
Authorized User	BROWN, J. ROBERT

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	11913-US-CNT3_2016-01-25_IDS.pdf	614837 e6b4f5d8872ca1187441b775e36a19b5ae187458	no	4
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Foreign Reference	WO2004053618A2.pdf	6174860 b6b65c9142b9b24c9aceae8f58ce297946b6b7d1	no	42
Warnings:					
Information:					
3	Non Patent Literature	RFC2459.pdf	244378 b18d927b38f501cdd2437268df48d92ff629dbc5	no	129
Warnings:					
Information:					
4	Other Reference-Patent/App/Search documents	EPSummons_25708_103015.pdf	898567 14978a4fd1027effb3f3c9bf3590ad6be365c377	no	6
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30810 8f764993281682edd1996430a4fed50419cc93d8	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	7963452		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2004053618	WO	A2	2004-06-24	Research In Motion Limited		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14715227
	Filing Date	2015-05-18
	First Named Inventor	Neil P. Adams
	Art Unit	2876
	Examiner Name	Daniel A. Hess
	Attorney Docket Number	11913-US-CNT3 4214-25714

	1	HOUSLEY, R., et al.; "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"; RFC 2459; January 1999; 129 pages.
	2	European Summons to Attend Oral Proceedings; Application No. 05739066.8; October 30, 2015; 6 pages. (4214-25708)

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2876
Examiner Name	Daniel A. Hess
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2016-01-25
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14715227
Filing Date:	18-May-2015
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	J. Robert Brown/Rami Law
Attorney Docket Number:	11913-US-CNT3 4214-25714

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

DO NOT ENTER: /D.A.H/

Attorney Docket No. 11913-US-CNT[3]
4214-25714

01/20/2016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: BlackBerry Limited	§	
	§	Group Art Unit: 2876
Application No.: 14/715,227	§	
	§	Examiner: Daniel A. Hess
Filed: May 18, 2015	§	
	§	Confirmation No.: 5874
For: SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES	§	

AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION DATED NOVEMBER 10, 2015

Commissioner:

In response to the Final Office Action dated November 10, 2015 in the above-identified application, the Applicant respectfully submits the following Amendment and Response. The changes made are shown by underlining the added text and striking through or double-bracketing the deleted text.

Amendments to the Claims are reflected in the listing of claims that begins on Page 2 of this paper.

Remarks begin on Page 10 of this paper.

Nintendo Exhibit 1003
Part 1 of 2
Page 00261

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714	5874

82313 7590 01/25/2016

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

EXAMINER	
HESS, DANIEL A	

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
01/25/2016	ELECTRONIC

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

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

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

ConleyRoseReporting@dfw.conleyrose.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 14/715,227	**Applicant(s)** ADAMS ET AL.	
	Examiner DANIEL HESS	**Art Unit** 2876	**AIA (First Inventor to File) Status** No

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

THE REPLY FILED 11 January 2016 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

   Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☒ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: *The examiner refers back to the final rejection, which addresses the limitations of the claims in considerable detail. The examiner maintains that even with the 1/11/2016 proposed amendments, the claim limitations are anticipated or rendered obvious by Fisher (of record) and the access control systems of Windows and other operating systems.*

   Regarding having the "owner control information in a protected data store" as per the 1/11/2016 proposed claim amendments, the examiner emphasizes that the Access Control Lists common to operating systems such as Windows and many others are a protected part of the operating system. A user cannot simply change Windows system files; users do not have this kind of access to system files. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): (a) ☐ will not be entered, or (b) ☐ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.
13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
14. ☐ Other:

/DANIEL HESS/
Primary Examiner, Art Unit 2876

Electronic Acknowledgement Receipt

EFS ID:	24587978
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Lesley Forte
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	11-JAN-2016
Filing Date:	18-MAY-2015
Time Stamp:	17:17:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		11913-US-CNT3_2016-01-11_RESP_OA2_Final.pdf	95729 f47275b21ec0918e64a845114e28b77bddd be070	yes	17

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Response After Final Action	1	1
	Claims	2	9
	Applicant Arguments/Remarks Made in an Amendment	10	17
Warnings:			
Information:			
	Total Files Size (in bytes):	95729	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: BlackBerry Limited	§	
	§	Group Art Unit: 2876
Application No.: 14/715,227	§	
	§	Examiner: Daniel A. Hess
Filed: May 18, 2015	§	
	§	Confirmation No.: 5874
For: SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES	§	

AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION DATED NOVEMBER 10, 2015

Commissioner:

In response to the Final Office Action dated November 10, 2015 in the above-identified application, the Applicant respectfully submits the following Amendment and Response. The changes made are shown by underlining the added text and striking through or double-bracketing the deleted text.

Amendments to the Claims are reflected in the listing of claims that begins on Page 2 of this paper.

Remarks begin on Page 10 of this paper.

REMARKS

The Final Office Action of November 10, 2015 has been carefully reviewed. The Applicant respectfully requests the Examiner to reconsider the rejections and allow the pending claims in view of the following remarks.

STATUS OF CLAIMS

Claims 1-3, 5-14, and 16-20 stand rejected. Claims 1, 5-8, 12, and 17-20 are hereby amended. Claims 4 and 15 were previously canceled. Claim 11 is hereby cancelled. Claims 21-23 are newly added. Therefore, claims 1-3, 5-10, 12-14, and 16-23 are pending. Support for the present amendments can be found at least in the original claims and paragraphs 66 and 73 of the specification.

REJECTION OF CLAIMS – 35 U.S.C. §§ 102 AND 103

In the Final Office Action mailed November 10, 2015, the Examiner rejected claims 1-3, 5, 9, 10, 12-14, 16, and 20 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication No. 2003/0101292 to Fisher, et al. ("Fisher").

Claims 6-8, 11, and 17-19 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher.

For convenience, the Applicant will address the claims at issue with respect to independent claim 1. Claim 1, as amended, recites:

> 1. A method of application control on an electronic device, the method comprising:
> **receiving, by the electronic device, owner information from an owner of the electronic device;**
> **receiving, by the electronic device, owner control information that identifies permissions associated with applications executable**

> **by the electronic device;**
>
> **storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information**;
>
> receiving, by the electronic device, from an application operating on the electronic device, a request to access the local memory on the electronic device;
>
> determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and
>
> controlling application access to the local memory based upon the determining.

(Emphasis added). The Applicant submits that the amended claim elements are not disclosed or rendered obvious by Fisher.

The Office Action alleges that "Fisher shows the principle whereby multiple users on a computer system and the applications associated with that user are granted access to certain local memory and barred access to other local memory." Office Action at p. 5. Fisher discloses that "to permit multiple users to access a single computer system, the various users (and their applications) are assigned various separate resources within the system." Fisher, ¶ 4. Specifically, Fisher discloses that "various memory addresses are assigned to one user application and various other memory addresses are assigned to another to avoid overlap" and "interference between applications." *Id.*

However, Fisher does not disclose separately receiving "owner information" and "owner control information," in which the "owner control information identifies permissions associated with applications executable by the electronic device," as claimed. Instead, Fisher generally discloses the idea of sandboxing whereby memory is partitioned among users and/or applications. *Id.* However, Fisher does not disclose two **separate steps of receiving** (1) owner information from an owner of the device and (2) owner control

information that details of how the local memory is partitioned for each user or application, as claimed (emphasis added).

Claim 1 also provides that the "owner control information" be stored in "a protected data store" to prevent alteration or deletion "in response to authenticating the owner control information using the owner information." The Office Action alleges:

> In the case of organization controlled IT, described above, regular users may not install or delete any application within their allocated space. This an administrative-level function. Users certainly can run applications and operate within applications to create and delete data files associated with those applications, but they may not control the installation and authorizations of applications. This is a protected data store.

Office Action, pp. 7-8. The Examiner asserts the above description based on the Examiner's personal experience or opinions as the claimed "protected data store." *Id.* However, this description does not qualify as prior art with respect to the present claims.

More specifically, the record is devoid of *factual* evidence that the information relied upon by the Examiner reflects "what a person of ordinary skill in the pertinent art would have known **at the time of the invention**." § MPEP 2141(II). At best, the information in the Examiner's description simply reflects what might be commonly known *today*, but there is no proof that such information was commonly known more than **ten years** ago when the invention was made.[1] As wireless technology has widely advanced at rapid rates[2] over the past decade, it cannot be presumed – without avoiding hindsight – that one of ordinary skill in the art would have known *at the time of the invention* that

[1] The present application is a continuation-in-part of U.S. Appl. No. 13/606,814, filed on September 7, 2012, which is a continuation of U.S. Appl. No. 12/869,589 filed on August 26, 2010, now U.S. Patent No. 8,302,185, which is a continuation of U.S. Appl. No. 10/732,132, filed on December 10, 2003, now U.S. Patent No. 7,793,355, which claims priority to U.S. Appl. No. 60/432,610, filed on December 12, 2002.

[2] *See* MPEP 2141 ("Factors that may be considered in determining the level of ordinary skill in the art may include…rapidity with which innovations are made").

Nintendo Exhibit 1003
Part 1 of 2
Page 00269

owner control information is received separately from owner information and stored in protected data store to prevent alteration or deletion of the owner control information. *See* MPEP § 2141.01 ("The requirement 'at the time the invention was made' is to avoid impermissible hindsight.")

Here, the only evidence to support such a presumption lies in the description above, which again is based on the Examiner's own understanding or experience. Yet this alone is not sufficient, as "the legal conclusion must be reached on the basis of the **facts gleaned from the prior art**." MPEP § 2142. Thus, the Examiner "must point to some **concrete evidence** in the record in support of these findings." MPEP § 2144.03(C). As previously mentioned, the record is devoid of any evidence to support the Examiner's finding of what was known *at the time of the invention* (e.g., in December of 2002). "If the [i]examiner is relying on personal knowledge to support the finding of what is known in the art, the examiner must provide an **affidavit or declaration setting forth specific factual statements and explanation to support the finding**." *Id.* Since no affidavit or declaration has been provided to support the Examiner's reliance on common knowledge in rejecting the claims, the Applicant respectfully submits that the outstanding claim rejections are not proper and should be withdrawn.

The Applicant further submits that Fisher does not disclose that (1) the owner control information is authenticated using the owner information and then (2) stored in "a protected data store," as claimed. While Fisher discloses that different applications are assigned different memory addresses, Fisher does not disclose that authentication of any information is performed before assigning applications different memory addresses, as claimed. In addition, Fisher does not disclose that "owner control information" indicating

Nintendo Exhibit 1003
Part 1 of 2
Page 00270

how the local memory is partitioned is stored in a "protected data store," as recited in amended claim 1. Therefore, Fisher does not disclose or render obvious at least the elements of amended claim 1 emphasized above.

In addition, under "Response to Amendments and Arguments," the Office Action further alleges:

> The examiner draws attention particularly to the 84 page prior art document already of record entitled "Managing Authorization and Access Control" (Windows XP Guide, Published: November 03, 2005 and made of record in the 6/4/2015 IDS, and which this examiner first brought to the attention of the applicants in an earlier application) which shows how access control works in Windows, the world's most common operating system.

Office Action at p. 2. The Applicant notes that the Windows XP Guide document referred to above ("Windows XP Guide") has not been asserted in the rejections of claims 1-3, 5-14, and 16-20. Instead, the Examiner merely references Windows XP Guide under the "Response to Amendments and Arguments" and states that the "[E]xaminer has referenced Microsoft Windows because it is the market-dominant operating system running on billions of computers worldwide, but the concepts in [Windows XP Guide] are broadly common across operating systems, and predate [W]indows." Office Action at p. 4.

The Examiner appears to be using the Windows XP Guide as an additional reference to reject the claims without officially asserting Windows XP Guide under § 102 or § 103. However, the Applicant submits that relying on Windows XP Guide as allegedly teaching the claimed features is improper because **Windows XP Guide does not constitute prior art** with respect to the present application. The present application claims priority to a U.S. provisional application No. 60/432,610 filed on **December 12, 2002**, which predates the publication date of Windows XP Guide, which is November 3,

Nintendo Exhibit 1003
Part 1 of 2
Page 00271

2005. *See* MPEP § 706. Therefore, the Windows XP Guide cannot support the level of knowledge in the art or otherwise be applied against the present claims because the Windows XP Guide was published after the present application was effectively filed.

The Office Action also alleges:

> The examiner emphasizes that the concept of ownership that Fisher refers to carries with it a tremendous amount of meaning, since the idea of permissions and rights is long established in the realm of operating systems. The examiner has referenced Microsoft Windows because it is the market-dominant operating system running on billions of computers worldwide, but the concepts in the document above are broadly common across operating systems, and predate windows.

Office Action at p. 4. As shown above, the Office Action makes a blanket allegation that the concepts in Windows XP Guide predate windows. The Applicant submits that the record is again devoid of **factual** evidence that the information relied upon by the Examiner reflects "what a person of ordinary skill in the pertinent art would have known **at the time of the invention**." § MPEP 2141(II). Again, the only evidence to support such a presumption allegedly lies in Windows XP Guide, which, as discussed above, does not constitute prior art. The "legal conclusion must be reached on the basis of the **facts gleaned from the prior art**." MPEP § 2142. Thus, the Examiner "must point to some **concrete evidence** in the record in support of these findings." MPEP § 2144.03(C). As previously mentioned, the record is devoid of any evidence to support the Examiner's finding of what was known *at the time of the invention* (e.g., in December of 2002). Since no affidavit or declaration has been provided to support the Examiner's reliance on common knowledge in rejecting the claims, the Applicant respectfully submits that the outstanding claim rejections are not proper and should be withdrawn.

Nintendo Exhibit 1003
Part 1 of 2
Page 00272

Therefore, claim 1, as amended, is not anticipated or rendered obvious by Fisher. Claims 12 and 20, as amended, recite similar elements to amended claim 1. Therefore, claims 12 and 20 are likewise not anticipated or rendered obvious by Fisher. Although Windows XP Guide does not constitute prior art, the Applicant submits that Windows XP Guide does not make up for the shortcomings of Fisher. For at least the foregoing reasons, the Applicant respectfully requests the Examiner to reconsider and withdraw the rejections of claims 1, 12, 20, and their dependent claims.

Nintendo Exhibit 1003
Part 1 of 2
Page 00273

CONCLUSION

The Applicant respectfully submits that the application, in its present form, is in condition for allowance. If the Examiner has any questions or comments or otherwise feels it would be helpful in expediting the application, the Examiner is encouraged to telephone the undersigned at (972) 731-2288. The Applicant intends this communication to be a complete response to the Final Office Action mailed November 10, 2015.

The Commissioner is hereby authorized to charge payment of any fee associated with any of the foregoing papers submitted herewith or any fees during the prosecution of the present case to Deposit Account No. 50-1515, Conley Rose, P.C.

Respectfully submitted,

CONLEY ROSE, P.C.

Date: January 11, 2016

/J. Robert Brown, Jr./
J. Robert Brown, Jr.
Reg. No. 45,438

ATTORNEY FOR APPLICANT

5601 Granite Parkway, Suite 500
Plano, Texas 75024
Telephone: (972) 731-2288
Facsimile: (972) 731-2289

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method of application control on an electronic device, the method comprising:

receiving, by the electronic device, owner information from an owner of the electronic device;

receiving, by the electronic device, owner control information that identifies permissions associated with applications executable by the electronic device;

storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;

determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information ~~based upon authorization record and an application identifier associated with the application, wherein the authorization record and the application identifier are included in owner control information stored on the electronic device for each application allowed to be executed on the electronic device, and wherein insertion of additional owner control information onto the electronic device is restricted~~; and

controlling application access to the local memory based upon the determining.

2. (Original) The method of claim 1, wherein the request to access the local memory comprises a request to erase data from the local memory.

3. (Original) The method of claim 1, wherein the request to access the local memory comprises a request to read data from the local memory.

4. (Canceled)

5. (Currently Amended) The method of claim 1, further comprising restricting modification of the owner control information after the owner control information has been stored ~~on the electronic device~~in the protected data store.

6. (Currently Amended) The method of claim 1, wherein the owner control information includes an authorization record and [[the]] an application identifier for each of the applications, and the owner control information is [[are]] provided by an external source through a wireless communication channel.

7. (Currently Amended) The method of claim [[1]] 6, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

8. (Currently Amended) The method of claim 1, wherein an update to the ~~authorization record~~owner control information is provided by an external source for storage on the electronic device.

9. (Original) The method of claim 1, wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device, the method further comprising:

receiving requests to access the local memory from a plurality of applications operating on the electronic device;

determining whether access to the local memory is allowed to be performed by their respective applications based upon the stored authorization records and the application identifiers that are respectively associated with the plurality of applications; and

controlling access by the plurality of applications to local memory based upon whether access to the local memory is allowed.

10. (Original) The method of claim 9, wherein a group containing two or more of the applications is associated with one of the authorization records.

11. (Canceled)

Nintendo Exhibit 1003
Part 1 of 2
Page 00277

12. (Currently Amended) A device, comprising:

a memory; and

a processor coupled with the memory and configured by instructions stored in the memory to:

receive owner information from an owner of the device;

receive owner control information that identifies permissions associated with applications executable by the device;

store the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receive, from an application operating on the electronic device, a request to access local memory on the electronic device;

determine whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information~~based upon an authorization record and an application identifier associated with the application, wherein the authorization record and the application identifier are included in owner control information stored on the electronic device for each application allowed to be executed on the electronic device, and wherein insertion of additional owner control information onto the electronic device is restricted~~; and

control application access to the local memory based upon the determining.

13. (Original) The device of claim 12, wherein the request to access the local memory comprises a request to erase data from the local memory.

14. (Original) The device of claim 12, wherein the request to access the local memory comprises a request to read data from the local memory.

15. (Canceled)

16. (Previously Presented) The device of claim 12, further comprising restricting modification of the owner control information after the owner control information has been stored on the electronic device.

17. (Currently Amended) The device of claim 12, wherein the owner control information includes an authorization record and [[the]] an application identifier for each of the applications, and wherein the owner control information is [[are]] provided by an external source through a wireless communication channel.

18. (Currently Amended) The device of claim [[12]] 17, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

Nintendo Exhibit 1003
Part 1 of 2
Page 00279

19. (Currently Amended) The device of claim 12, wherein an update to the ~~authorization record~~owner control information is provided by an external source for storage on the electronic device.

Nintendo Exhibit 1003
Part 1 of 2
Page 00280

20. (Currently Amended) A non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the ~~steps~~ operations of:

receiving owner information from an owner of an electronic device;

receiving owner control information that identifies permissions associated with applications executable by the electronic device;

storing the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receiving, from an application operating on the electronic device, a request to access local memory on the electronic device;

determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information ~~based upon an authorization record and an application identifier associated with the application, wherein the authorization record and the application identifier are included in owner control information stored on the electronic device for each application allowed to be executed on the electronic device, and wherein insertion of additional owner control information onto the electronic device is restricted~~; and

controlling application access to the local memory based upon the determining.

21. (New) The non-transitory computer-readable medium of claim 20, wherein the owner control information includes an authentication record and an identifier for each application allowed to be executed on the electronic device.

22. (New) The non-transitory computer-readable medium of claim 20, wherein the request to access the local memory comprises a request to erase data from the local memory.

23. (New) The non-transitory computer-readable medium of claim 20, wherein the request to access the local memory comprises a request to read data from the local memory.

Nintendo Exhibit 1003
Part 1 of 2
Page 00282

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14715227	ADAMS ET AL.
	Examiner	**Art Unit**
	DANIEL HESS	2876

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/27/2015	11/03/2015							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	-							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	-							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14715227	ADAMS ET AL.
	Examiner	Art Unit
	DANIEL HESS	2876

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	375, 380	6/27/2015	DH
719	328		

SEARCH NOTES		
Search Notes	Date	Examiner
East keyword searches attached	6/27/2015	DH

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714	5874

82313 7590 11/10/2015

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

EXAMINER	
HESS, DANIEL A	

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
11/10/2015	ELECTRONIC

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

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

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

ConleyRoseReporting@dfw.conleyrose.com

Office Action Summary	Application No. 14/715,227	Applicant(s) ADAMS ET AL.	
	Examiner DANIEL HESS	Art Unit 2876	AIA (First Inventor to File) Status No

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

Period for Reply

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

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

Status

1)☒ Responsive to communication(s) filed on *10/8/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

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

Disposition of Claims*

5)☒ Claim(s) *1-3,5-14 and 16-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-3, 5-14, 16-20* is/are rejected.

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

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

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

Application Papers

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

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

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

The present application is being examined under the pre-AIA first to invent provisions. This action is responsive to applicant's amendments and arguments of 10/8/2015, which have been entered into the electronic file of record.

Response to Amendments and Arguments

Fisher refers to "users and their applications" throughout, especially at para 0004. Implicit in this is the reality that applications are associated with users and belong to users, as all files do.

The examiner draws attention particularly to the 84 page prior art document already of record entitled "Managing Authorization and Access Control" (Windows XP Guide, Published: November 03, 2005 and made of record in the 6/4/2015 IDS, and which this examiner first brought to the attention of the applicants in an earlier application) which shows how access control works in Windows, the world's most common operating system.

Among the teachings of that document:

From page 4,

"Owner

The only security principal who has an inherent right to allow or deny permission to access an object. An object's owner can give another security principal permission to take

ownership. By default, the built-in Administrators group on a computer is assigned a user right that allows this group to take ownership of all objects on the computer.

Security descriptor

A data structure containing the security information associated with a securable object. A security descriptor identifies an object's owner by SID. If permissions are configured for the object, its security descriptor contains a discretionary access control list (DACL) with SIDs for the users and groups that are allowed or denied access. If auditing is configured for the object, its security descriptor also contains a system access control list (SACL) that controls how the security subsystem audits attempts to access the object.

Access control list (ACL)

An ordered list of access control entries (ACEs) that define the permissions that apply to an object and Its properties. Each ACE identifies a security principal and specifies a set of access rights allowed, denied, or audited for that security principal."

If a user installs an application in their partition in Fisher, one of ordinary skill in the art would understand that they are the owner. Other than a system administration (if any), access by others is restricted. Others cannot gain ownership or control of an application without such being granted by the owner.

The applicant should carefully review the above document, which discusses owners and file permissions in many, many places. This document shows generally how operating systems manage rights and controls of files. It becomes apparent that operating systems have built in

restrictions, and where individual users have full permissions of their own files and applications and other users on the same level (not counting administrations) do not have any rights on those files unless granted such by the owner.

The examiner emphasizes that the concept of ownership that Fisher refers to carries with it a tremendous amount of meaning, since the idea of permissions and rights is long established in the realm of operating systems. The examiner has referenced Microsoft Windows because it is the market-dominant operating system running on billions of computers worldwide, but the concepts in the document above are broadly common across operating systems, and predate windows.

Access Control Lists in particular should be studied closely. They are conventional across most operating systems including Unix based systems and systems by Apple.

Claim Rejections - 35 USC § 102

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

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5, 9, 10, 12-14, 16 and 20 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Fisher et al. (US 2003/0101292).

Re claim 1, 5:

Fisher applies to an electronic device.

Fisher teachs at para [0004]:

"**In order to permit multiple users to access a single computer system, the various users (and their applications) are assigned various separate resources within the system.** For instance, **various memory addresses are assigned to one user application** and various other memory addresses are assigned to another to avoid overlap. This is known in the art as sandboxing. Such separation is used to avoid interference between applications that can cause undesired effects to occur."

Fisher teaches at para [0006]:

"**Substantially all multiprogrammed systems rely upon software and/or hardware solutions that prevent applications from accessing memory addresses that are out of the permissible range.** The software solutions typically at least statically review the instructions of a particular application when it is loaded to determine whether any of the instructions contain a direct memory reference to an out-of-range memory address."

Fisher shows the principle whereby multiple users on a computer system and the applications associated with that user are granted access to certain local memory and barred access to other local memory. This achieves several ends as the above excerpt demonstrates:

(1) Memory can be allocated to users and their applications can only use the memory that belongs to their owners.

(2) A first application cannot access and interfere with the memory of a second different application, possibly by a different user.

In keeping with the above, application identifiers would be associated with user identifiers and memory is associated with user identifiers. Users of a system in turn would have their own authorizations to be able to access the system and applications gain authorization to access certain memory through those users.

It is noted that this principle of delineated memory seen above applies both on a larger level to user accounts and on a finer level to multiple applications belonging to the same user.

"Insertion of additional owner information" would be restricted at least in the sense that another user on the same level could not on their own obtain access to memory and applications belonging to a different user. That is the meaning of assigning users control. See discussions above.

Re claims 2 and 3: Memory access by an application as described above generally includes all of read, write and erase ability.

Re claims 9 and 10: Fisher clearly can apply (as seen in the excerpt above) to user accounts that may have multiple applications in them. The authorization record, which is associated with one user, applies to two or more applications.

Re claims 12-14, 16: See discussions re claims 1-3, above.

Re claim 20: See discussion re claim 1 above.

Claim Rejections - 35 USC § 103

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

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

Claims 6-8, 11 and 17-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over by Fisher et al.

Re claim 6: See para 0039, where it is seen that the system in question can be a server computer. Server computers are conventionally accessed remotely for both control and providing service to clients. Wireless networks could reasonably be part of the remote access configuration in Fisher et al.

Re claims 7 and 8: Claims 1 and 7 to a good approximation describe the configuration that has been present at the USPTO since prior to the instant invention. An external server system managed by the USPTO administers all policies. Specifically the server supplies users with access to applications and pushes applications for users. Users have specifically allocated memory on servers for their accounts and to be used by their application.

This is similar to what is seen in paragraphs 0004 and 0006 of Fisher, but with organizational control.

Re claim 11: In the case of organization controlled IT, described above, regular users may not install or delete any application within their allocated space. This an administrative-level

function. Users certainly can run applications and operate within applications to create and delete data files associated with those applications, but they may not control the installation and authorizations of applications. This is a protected data store.

Re claims 17-19: See discussion re claims 6-8, above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANIEL HESS whose telephone number is (571)272-2392. The examiner can normally be reached on 9:00 AM - 5:00 PM M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/DANIEL HESS/

Primary Examiner, Art Unit 2876

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method of application control on an electronic device, the method comprising:

receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;

determining whether the application is allowed to access the local memory based upon an authorization record and an application identifier associated with the application, wherein the authorization record and the application identifier are included in owner control information stored on the electronic device for each application allowed to be executed on the electronic device, and wherein insertion of additional owner control information onto the electronic device is restricted; and

controlling application access to the local memory based upon the determining.

2. (Original) The method of claim 1, wherein the request to access the local memory comprises a request to erase data from the local memory.

3. (Original) The method of claim 1, wherein the request to access the local memory comprises a request to read data from the local memory.

4. (Canceled)

Nintendo Exhibit 1003
Part 1 of 2
Page 00295

5. (Currently Amended) The method of claim [[4]] 1, further comprising restricting modification of the owner control information after the owner control information has been stored on the electronic device.

6. (Original) The method of claim 1, wherein the authorization record and the application identifier are provided by an external source through a wireless communication channel.

7. (Original) The method of claim 1, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

8. (Original) The method of claim 1, wherein an update to the authorization record is provided by an external source for storage on the electronic device.

Nintendo Exhibit 1003
Part 1 of 2
Page 00296

9. (Original) The method of claim 1, wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device, the method further comprising:

receiving requests to access the local memory from a plurality of applications operating on the electronic device;

determining whether access to the local memory is allowed to be performed by their respective applications based upon the stored authorization records and the application identifiers that are respectively associated with the plurality of applications; and

controlling access by the plurality of applications to local memory based upon whether access to the local memory is allowed.

10. (Original) The method of claim 9, wherein a group containing two or more of the applications is associated with one of the authorization records.

11. (Original) The method of claim 1, wherein the authorization record is stored in a protected data store, thereby preventing alteration or deletion of the authorization record unless permitted.

Nintendo Exhibit 1003
Part 1 of 2
Page 00297

12. (Currently Amended) A device, comprising:

a memory; and

a processor coupled with the memory and configured by instructions stored in the memory to:

receive, from an application operating on the electronic device, a request to access local memory on the electronic device;

determine whether the application is allowed to access the local memory based upon an authorization record and an application identifier associated with the application, wherein the authorization record and the application identifier are included in owner control information stored on the electronic device for each application allowed to be executed on the electronic device, and wherein insertion of additional owner control information onto the electronic device is restricted; and

control application access to the local memory based upon the determining.

13. (Original) The device of claim 12, wherein the request to access the local memory comprises a request to erase data from the local memory.

14. (Original) The device of claim 12, wherein the request to access the local memory comprises a request to read data from the local memory.

15. (Canceled)

16. (Currently Amended) The device of claim [[15]] 12, further comprising restricting modification of the owner control information after the owner control information has been stored on the electronic device.

17. (Original) The device of claim 12, wherein the authorization record and the application identifier are provided by an external source through a wireless communication channel.

18. (Original) The device of claim 12, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

19. (Original) The device of claim 12, wherein an update to the authorization record is provided by an external source for storage on the electronic device.

Nintendo Exhibit 1003
Part 1 of 2
Page 00299

20. (Currently Amended) A non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the steps of:

receiving, from an application operating on the electronic device, a request to access local memory on the electronic device;

determining whether the application is allowed to access the local memory based upon an authorization record and an application identifier associated with the application, wherein the authorization record and the application identifier are included in owner control information stored on the electronic device for each application allowed to be executed on the electronic device, and wherein insertion of additional owner control information onto the electronic device is restricted; and

controlling application access to the local memory based upon the determining.

Nintendo Exhibit 1003
Part 1 of 2
Page 00300

Electronic Acknowledgement Receipt

EFS ID:	23735617
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Rami Law
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	08-OCT-2015
Filing Date:	18-MAY-2015
Time Stamp:	17:26:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		11913-US-CNT3_2015-10-08_RESP_OA1.pdf	41274 643e21634ae6be9a1d9bbc4304ddc2edab7c3a16	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	12
Warnings:			
Information:			
	Total Files Size (in bytes):	41274	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

REMARKS

The Office Action of July 8, 2015 has been carefully reviewed. The Applicant respectfully requests the Examiner to reconsider the rejections and allow the pending claims in view of the following remarks.

STATUS OF CLAIMS

Claims 1-20 stand rejected. Claims 1, 5, 12, 16, and 20 are hereby amended. Claims 4 and 15 are hereby canceled without prejudice. Therefore, claims 1-3, 5-14, 16-20 and are pending. Support for the present amendments can be found at least in the original claims. No new matter is added.

TELEPHONE INTERVIEW

The Applicant thanks the Examiner for participating in the telephone interview on September 23, 2015. The substance of the interview is substantially the same as discussed herein.

REJECTION OF CLAIMS – 35 U.S.C. §§ 102 AND 103

In the Office Action mailed July 8, 2015, the Examiner rejected claims 1-5, 9, 10, 12-16, and 20 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication No. 2003/0101292 to Fisher ("Fisher").

Claims 6-8, 11, and 17-19 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher.

Nintendo Exhibit 1003
Part 1 of 2
Page 00303

For convenience, the Applicant will address the claims at issue with respect to claim 1. Independent claim 1, as amended, recites:

> A method of application control on an electronic device, the method comprising:
>
> receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;
>
> determining whether the application is allowed to access the local memory based upon an authorization record and an application identifier associated with the application, ***wherein the authorization record and the application identifier are included in owner control information stored on the electronic device for each application allowed to be executed on the electronic device, and wherein insertion of additional owner control information onto the electronic device is restricted***; and
>
> controlling application access to the local memory based upon the determining.

(Emphasis added). Independent claim has been amended to recite "wherein the authorization record and the application identifier are included in owner control information stored on the electronic device for each application allowed to be executed on the electronic device, and wherein insertion of additional owner control information onto the electronic device is restricted," as recited in previously presented, herein canceled, claim 4. Independent claims 12 and 20 have been amended to recite similar elements. The Applicant submits that Fisher does not disclose at least this element of amended claim 1.

The Office Action alleges that Fisher teaches that a "first application cannot access and interfere with the memory of a second different application, possibly by a different user." Office Action, p. 3. Specifically, the Office Action refers to paragraph 6 of Fisher, which states that "[s]ubstantially all multiprogrammed systems rely upon software and/or

hardware solutions that prevent applications from accessing memory addresses that are out of the permissible range." Fisher, ¶ 6. The Office Action further alleges:

> "Insertion of additional owner information" would be restricted at least in the sense that another user on the same level could not on their own obtain access to memory and applications belonging to a different user. That is the meaning of assigning users control.

Office Action, p. 3. The Applicant respectfully disagrees.

Fishes discloses a system and method for isolating applications executing on a multiprogrammed system from each other as to avoid interference between the applications. Fisher, ¶ 17. While Fisher generally discloses preventing applications from accessing memory addresses that are out of permissible range (Fisher, ¶ 6), Fisher does not disclose that such prevention is performed using owner control information that includes **an authorization record and an application identifier**, as claimed. (Emphasis added).

In addition, Fisher does not disclose "additional owner control information" wherein "insertion of [the] additional owner control information onto the electronic device is restricted," as recited in amended claim 1. As quoted above, the Office Action appears to allege that the claimed "insertion of additional owner control information" is the same as restricting access to memory and applications belonging to a different user. Office Action, p. 3. Even assuming, for the sake of argument, that Fisher were to disclose that users are restricted from accessing memory and applications belonging to other users, as alleged, this is not the same as restricting the **insertion of additional owner control information <u>onto the electronic device</u>**, as claimed. (Emphasis added). In fact, Fisher is silent regarding inserting additional owner control information onto the electronic device, much less restricting the insertion of the owner control information.

Therefore, claim 1, as amended, is not anticipated or rendered obvious by Fisher. Claims 12 and 20, as amended, recite similar elements to amended claim 1. Therefore, claims 12 and 20 are likewise not anticipated or rendered obvious by Fisher. For at least the foregoing reasons, the Applicant respectfully requests the Examiner to reconsider and withdraw the rejections of claims 1, 12, 20, and their dependent claims.

CONCLUSION

The Applicant respectfully submits that the application, in its present form, is in condition for allowance. If the Examiner has any questions or comments or otherwise feels it would be helpful in expediting the application, the Examiner is encouraged to telephone the undersigned at (972) 731-2288. The Applicant intends this communication to be a complete response to the Office Action mailed July 8, 2015.

The Commissioner is hereby authorized to charge payment of any fee associated with any of the foregoing papers submitted herewith or any fees during the prosecution of the present case to Deposit Account No. 50-1515, Conley Rose, P.C.

Respectfully submitted,

CONLEY ROSE, P.C.

Date: October 8, 2015

/J. Robert Brown, Jr./
J. Robert Brown, Jr.
Reg. No. 45,438

ATTORNEY FOR APPLICANT

5601 Granite Parkway, Suite 500
Plano, Texas 75024
Telephone: (972) 731-2288
Facsimile: (972) 731-2289

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	BlackBerry Limited	§	
		§	Group Art Unit: 2876
Application No.:	14/715,227	§	
		§	Examiner: Daniel A. Hess
Filed:	May 18, 2015	§	
		§	Confirmation No.: 5874
For:	SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES	§	

AMENDMENT AND RESPONSE TO
OFFICE ACTION DATED JULY 8, 2015

Commissioner:

In response to the Office Action dated July 8, 2015 in the above-identified application, the Applicant respectfully submits the following Amendment and Response. The changes made are shown by underlining the added text and striking through or double-bracketing the deleted text.

Amendments to the Claims are reflected in the listing of claims that begins on Page 2 of this paper.

Remarks begin on Page 8 of this paper.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/715,227	Filing Date 05/18/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	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 $310 ($155 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))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **10/08/2015**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 18	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					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.

LIE
/Theresa Dawkins/

This collection of information is required by 37 CFR 1.16. 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 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714

CONFIRMATION NO. 5874

82313
Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

PUBLICATION NOTICE

OC000000077351085

Title: System and Method of Owner Application Control of Electronic Devices

Publication No.US-2015-0254472-A1
Publication Date:09/10/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

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

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 5874

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/715,227	05/18/2015	235	2876	11913-US-CNT3 4214-25714

APPLICANTS

BlackBerry Limited, Waterloo, CANADA;

INVENTORS

Neil P. Adams, Kitchener, CANADA;
Michael G. Kirkup, Waterloo, CANADA;
Herbert A. Little, Waterloo, CANADA;
Russell N. Owen, Waterloo, CANADA;

**** CONTINUING DATA ***************************

This application is a CON of 13/618,311 09/14/2012 PAT 9033216
which is a CON of 12/885,281 09/17/2010 PAT 8887988
which is a CON of 11/118,844 04/29/2005 PAT 7815100
which claims benefit of 60/567,163 04/30/2004
This application 14/715,227 05/18/2015
is a CIP of 13/606,814 09/07/2012 ABN
which is a CON of 12/869,589 08/26/2010 PAT 8302185
which is a CON of 10/732,132 12/10/2003 PAT 7793355
which claims benefit of 60/432,610 12/12/2002

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

05/27/2015

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged // Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CANADA	9	20	3

ADDRESS

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024
UNITED STATES

TITLE

System and Method of Owner Application Control of Electronic Devices

FILING FEE RECEIVED		
1740	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____

BIB (Rev. 05/07).

Notice of References Cited	Application/Control No. 14/715,227	Applicant(s)/Patent Under Reexamination ADAMS ET AL.	
	Examiner DANIEL HESS	Art Unit 2876	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0101292	05-2003	Fisher et al.	709/328
*	B	US-2004/0210760	10-2004	McGrath et al.	713/190
*	C	US-5,784,552	07-1998	Bishop et al.	714/38.12
*	D	US-2003/0178482	09-2003	Kisliakov, Andrew	235/380
	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.

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown /DANIEL HESS/
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5560008		1996-09-24	Johnson, et al.	
	2	5619710		1997-04-08	Travis, Jr., et al.	
	3	5778348		1998-07-07	Manduley, et al.	
	4	5944821		1999-08-31	Angelo	
	5	6061794		2000-05-09	Angelo, et al.	
	6	6101607		2000-08-08	Bachand, et al.	
	7	6134659		2000-10-17	Sprong, et al.	
	8	6134593		2000-10-17	Alexander, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	9	6141754		2000-10-31	Choy	
	10	6167521		2000-12-26	Smith, et al.	
	11	6192476	B1	2001-02-20	Gong	
	12	6202207	B1	2011-03-13	Donohue	
	13	6212635	B1	2001-04-03	Reardon	
	14	6216116	B1	2001-04-10	Barkan, et al.	
	15	6233608	B1	2001-05-15	Laursen, et al.	
	16	6480961	B2	2002-11-12	Rajasekharan, et al.	
	17	6487665	B1	2002-11-26	Andrew, et al.	
	18	6513121	B1	2003-01-28	Serkowski	
	19	6922782	B1	2005-07-26	Spyker, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	20	6931379	B1	2005-08-16	Sato, et al.	
	21	7546956	B2	2009-06-16	Adams, et al.	
	22	7793355	B2	2010-09-07	Little, et al.	
	23	7815100	B2	2010-10-19	Adams, et al.	
	24	8302185	B2	2012-10-30	Little, et al.	
	25	8429410	B2	2013-04-23	Little, et al.	
	26	8887988	B2	2014-11-18	Adams, et al.	
	27	9033216	B2	2015-05-19	Adams, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010002485	A1	2001-05-31	Bisbee, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	2	20010032188	A1	2001-10-18	Miyabe, et al.	
	3	20020007454	A1	2002-01-17	Tarpenning, et al.	
	4	20020152376	A1	2002-10-17	Eigeles	
	5	20030172034	A1	2003-09-11	Schneck, et al.	
	6	20030191719	A1	2003-10-09	Ginter, et al.	
	7	20040039911	A1	2004-02-26	Oka, et al.	
	8	20040078565	A1	2004-22-04	Hofmeister, et al.	
	9	20050050319	A1	2005-03-03	Suraski	
	10	20060272028	A1	2006-11-30	Maes	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	1	0384610	EP	A2	1992-02-06	International Business Machines		☐
	2	2312767	GB	A	1997-11-05	Mitel Corporation		☐
	3	0828209	EP	A2	1998-03-11	Samsung Electronics, Ltd.		☐
	4	1998044404	WO	A1	1998-10-08	Sun Mircrosystems, Inc.		☐
	5	0060434	WO	A1	2000-10-12	Microsoft Corporation		☐
	6	2355819	GB	A	2001-05-02	Marconi Communications United		☐
	7	2001171590	WO	A1	2001-09-27	Vasara Research, Inc.		☐
	8	2001077811	WO	A1	2001-10-18	Everdream, Inc.		☐
	9	1168141	EP	A2	2002-01-02	Franklin Electronic Publishers, Inc.		☐
	10	2002056360	JP	A	2002-02-20	Hitachi, Ltd.		☒
	11	2002091598	JP	A	2002-03-29	Nippon Computer Co., Ltd.		☒

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	12	2002170063	JP	A	2002-06-14	NTT Communications		☒
	13	2002182963	JP	A	2002-06-28	Ricoh Co., Ltd.		☒
	14	2002097620	WO	A2	2002-12-05	Qualcomm Incorporated		☐
	15	2825565	FR	A1	2002-12-06	Sagem		☒
	16	2378780	GB	A	2003-02-19	Elan Digital Systems Limited		☐
	17	2333865	GB	B	2003-05-14	International Business Machines Corp.		☐
	18	2003058411	WO	A1	2003-07-17	NTT Docomo, Inc.		☐
	19	2003063524	WO	A1	2003-07-31	Yahoo, Inc.		☐
	20	1185923	EP	B1	2004-03-31	Elata Limited		☐
	21	1427166	EP	A2	2004-06-09	Canon Kabushiki Kaisha		☐
	22	1465041	EP	A2	2004-10-06	NTT Docomo, Inc.		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	23	0813132	EP	B1	2005-01-26	International Business Machines Corporation		☐
	24	2429148	EP	A2	2012-03-14	NTT DoCoMo, Inc.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	TAKARAGI; "Angou Houshiki to Ouyou [Encryption system and Application]"; Journal of Information Processing; Volume 32, No. 6; Japan: Information Processing Society of Japan; June 1991; 11 pages. (as referenced in Japanese Office Action dated February 10, 2009 for Application No. 2004-557718)	☐
	2	BOS, BERT; "Re: CSS: Extended Tiling. Proposal"; www-style@w3.org, http://lists.w3.org/Archives/Public/www-style/2004May/0020.html; May 5, 2004; 2 pages.	☐
	3	W3C; "CSS3 Module: Border"; http://www.w3.org/TR/2002/WD-css3-border-20021107/ November 7, 2002; 14 pages.	☐
	4	W3C; "CSS3 Backgrounds and Borders Module"; www.w3.org/TR/2005/WD-css3-background-20050216/; February 16, 2005; 30 pages.	☐
	5	SAMARATI, Pierangela, et al.; "Access Control: Policies, Models, and Mechanisms"; Foundations of Security Analysis and Design; Lecture Notes in Computer Science Volume 2171; 2001; 60 pages.	☐
	6	Microsoft; "Managing Authorization and Access Control"; http://technet.microsoft.com/en-us/library/bb457115.aspx; November 3, 2005; 84 pages.	☐
	7	CLARKSON, Michael; "Access Control"; http://www.cs.cornell.edu/courses/cs513/2007fa/NL.accessControl.html; 2007; 8 pages.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	8	Wikipedia; "Access Control List"; http://en.wikipedia.org/wiki/Access_control_list; retrieved July 2, 2013; 3 pages.	☐
	9	Wikipedia; "Access Control List"; http://en.wikipedia.org/wiki/Access_control_list; retrieved June 5, 2013; 1 page.	☐
	10	Office Action dated August 21, 2007; U.S. Application No. 10/784,024 filed February 20, 2004; 21 pages. 10802-US-PAT	☐
	11	Office Action dated June 11, 2007; U.S. Application No. 10/732,132 filed December 10, 2003; 13 pages. (4214-27101)	☐
	12	Office Action dated February 22, 2008; U.S. Application No. 10/732,132 filed December 10, 2003; 11 pages. (4214-27101)	☐
	13	Final Office Action dated September 23, 2008; U.S. Application No. 10/732,132 filed December 10, 2003; 9 pages. (4214-27101)	☐
	14	Advisory Action dated December 8, 2008; U.S. Application No. 10/732,132 filed December 10, 2003; 3 pages. (4214-27101)	☐
	15	Office Action dated April 2, 2009; U.S. Application No. 10/732,132 filed December 10, 2003; 10 pages. (4214-27101)	☐
	16	Final Office Action dated October 28, 2009; U.S. Application No. 10/732,132 filed December 10, 2003; 10 pages. (4214-27101)	☐
	17	Advisory Action dated January 19, 2010; U.S. Application No. 10/732,132 filed December 10, 2003; 3 pages. (4214-27101)	☐
	18	Notice of Allowance dated May 4, 2010; U.S. Application No. 10/732,132 filed December 10, 2003; 7 pages. (4214-27101)	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	19	Office Action dated August 3, 2011; U.S. Application No. 12/869,589 filed August 26, 2010; 20 pages. (4214-27115)	☐
	20	Office Action dated January 19, 2012; U.S. Application No. 12/869,589 filed August 26, 2010; 11 pages. (4214-27115)	☐
	21	Notice of Allowance dated June 13, 2012; U.S. Application No. 12/869,589 filed August 26, 2010; 9 pages. (4214-27115)	☐
	22	Office Action dated June 17, 2013; U.S. Application No. 13/606,814 filed September 7, 2012; 19 pages. (4214-27116)	☐
	23	Final Office Action dated October 10, 2013; U.S. Application No. 13/606,814 filed September 7, 2012; 6 pages. (4214-27116)	☐
	24	Office Action dated May 29, 2008; U.S. Application No. 11/118,844 filed April 29, 2005; 4 pages. (4214-25701)	☐
	25	Office Action dated March 10, 2009; U.S. Application No. 11/118,844 filed April 29, 2005; 6 pages. (4214-25701)	☐
	26	Office Action dated August 20, 2009; U.S. Application No. 11/118,844 filed April 29, 2005; 15 pages. (4214-25701)	☐
	27	Notice of Allowance dated February 23, 2010; U.S. Application No. 11/118,844 filed April 29, 2005; 7 pages. (4214-25701)	☐
	28	Notice of Allowance dated June 10, 2010; U.S. Application No. 11/118,844 filed April 29, 2005; 8 pages. (4214-25701)	☐
	29	Office Action dated April 7, 2008; U.S. Application No. 11/118,748 filed April 29, 2005; 11 pages. (4214-25702)	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	30	Final Office Action dated October 27, 2008; U.S. Application No. 11/118,748 filed April 29, 2005; 10 pages. (4214-25702)	☐
	31	Notice of Allowance dated February 9, 2009; U.S. Application No. 11/118,748 filed April 29, 2005; 6 pages. (4214-25702)	☐
	32	Office Action dated March 22, 2010; U.S. Application No. 12/468,441 filed May 19, 2009; 12 pages. (4214-25703)	☐
	33	Notice of Allowance dated August 11, 2010; U.S. Application No. 12/468,441 filed May 19, 2009; 12 pages. (4214-25703)	☐
	34	Office Action dated November 12, 2013; U.S. Application No. 12/885,281 filed September 17, 2010; 32 pages. (4214-25712)	☐
	35	Office Action dated April 3, 2014; U.S. Application No. 12/885,281 filed September 17, 2010; 9 pages. (4214-25712)	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DANIEL HESS/	Date Considered	06/27/2015

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2015-06-04
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14715227	ADAMS ET AL.
	Examiner	Art Unit
	DANIEL HESS	2876

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/27/2015								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S20	192	adams.in. and neil.in. and (application with control)	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:47
S21	419	adams.in. and neil.in. and (application near4 control)	US-PGPUB; USPAT	OR	ON	2015/06/26 15:47
S22	295	adams.in. and neil.in. and (application adj control)	US-PGPUB; USPAT	OR	ON	2015/06/26 15:47
S23	38	adams.in. and neil.in. and (application adj control)	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:47
S24	35	S23 and (electronic adj devic$2)	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:48
S25	0	S24 and (access adj2 memory).clm.	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:48
S26	0	S24 and (access adj4 memory).clm.	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:48
S27	35	S24 and (access adj4 memory)	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:48
S28	37	("20010002485" | "20010032188" | "20020007454" | "20020152376" | "20030172034" | "20030191719" | "20040039911" | "20040078565" | "20050050319" | "20060272028" | "5560008" | "5619710" | "5778348" | "5944821" | "6061794" | "6101607" | "6134593" | "6134659" | "6141754" | "6167521" | "6192476" | "6202207" | "6212635" | "6216116" | "6233608" | "6480961" | "6487665" | "6513121" | "6922782" | "6931379" | "7546956" | "7793355" | "7815100" | "8302185" | "8429410" | "8887988" | "9033216").PN.	US-PGPUB; USPAT	OR	OFF	2015/06/26 16:00
S29	32	S28 not adams.in.	US-PGPUB; USPAT	OR	OFF	2015/06/26 16:01
S30	14	S29 and (access$4 near3 memory)	US-PGPUB; USPAT	OR	OFF	2015/06/26 16:01
S31	1	(permission same application same (access adj local adj memory))	US-PGPUB; USPAT	OR	OFF	2015/06/26 16:09
S32	1	(right same application same (access adj local	US-	OR	OFF	2015/06/26

Nintendo Exhibit 1003
Part 1 of 2
Page 00326

		adj memory))	PGPUB; USPAT			16:09
S33	12	((permission or right) same application same (access$3 adj local adj memory))	US-PGPUB; USPAT	OR	ON	2015/06/26 16:10
S34	207	(prevent$4 near2 application near4 access$5 near2 memory)	US-PGPUB; USPAT	OR	ON	2015/06/26 16:24

EAST Search History (Interference)

<This search history is empty>

6/27/2015 12:53:37 PM

Nintendo Exhibit 1003
Part 1 of 2
Page 00327

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	192	adams.in. and neil.in. and (application with control)	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:47
L2	419	adams.in. and neil.in. and (application near4 control)	US-PGPUB; USPAT	OR	ON	2015/06/26 15:47
L3	295	adams.in. and neil.in. and (application adj control)	US-PGPUB; USPAT	OR	ON	2015/06/26 15:47
L4	38	adams.in. and neil.in. and (application adj control)	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:47
L5	35	4 and (electronic adj devic$2)	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:48
L6	0	5 and (access adj2 memory).clm.	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:48
L7	0	5 and (access adj4 memory).clm.	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:48
L8	35	5 and (access adj4 memory)	US-PGPUB; USPAT	OR	OFF	2015/06/26 15:48
L9	37	("20010002485" | "20010032188" | "20020007454" | "20020152376" | "20030172034" | "20030191719" | "20040039911" | "20040078565" | "20050050319" | "20060272028" | "5560008" | "5619710" | "5778348" | "5944821" | "6061794" | "6101607" | "6134593" | "6134659" | "6141754" | "6167521" | "6192476" | "6202207" | "6212635" | "6216116" | "6233608" | "6480961" | "6487665" | "6513121" | "6922782" | "6931379" | "7546956" | "7793355" | "7815100" | "8302185" | "8429410" | "8887988" | "9033216").PN.	US-PGPUB; USPAT	OR	OFF	2015/06/26 16:00
L10	32	9 not adams.in.	US-PGPUB; USPAT	OR	OFF	2015/06/26 16:01
L11	14	10 and (access$4 near3 memory)	US-PGPUB; USPAT	OR	OFF	2015/06/26 16:01
L12	1	(permission same application same (access adj local adj memory))	US-PGPUB; USPAT	OR	OFF	2015/06/26 16:09
L13	1	(right same application same (access adj local	US-	OR	OFF	2015/06/26

Nintendo Exhibit 1003
Part 1 of 2
Page 00328

		adj memory))	PGPUB; USPAT			16:09
L14	12	((permission or right) same application same (access$3 adj local adj memory))	US-PGPUB; USPAT	OR	ON	2015/06/26 16:10

EAST Search History (Interference)

<This search history is empty>

6/26/2015 4:10:43 PM

Nintendo Exhibit 1003
Part 1 of 2
Page 00329

Receipt date: 06/04/2015
Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

14715227 - GAU: 2876

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown /DANIEL HESS/
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5560008		1996-09-24	Johnson, et al.	
	2	5619710		1997-04-08	Travis, Jr., et al.	
	3	5778348		1998-07-07	Manduley, et al.	
	4	5944821		1999-08-31	Angelo	
	5	6061794		2000-05-09	Angelo, et al.	
	6	6101607		2000-08-08	Bachand, et al.	
	7	6134659		2000-10-17	Sprong, et al.	
	8	6134593		2000-10-17	Alexander, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	9	6141754		2000-10-31	Choy	
	10	6167521		2000-12-26	Smith, et al.	
	11	6192476	B1	2001-02-20	Gong	
	12	6202207	B1	2011-03-13	Donohue	
	13	6212635	B1	2001-04-03	Reardon	
	14	6216116	B1	2001-04-10	Barkan, et al.	
	15	6233608	B1	2001-05-15	Laursen, et al.	
	16	6480961	B2	2002-11-12	Rajasekharan, et al.	
	17	6487665	B1	2002-11-26	Andrew, et al.	
	18	6513121	B1	2003-01-28	Serkowski	
	19	6922782	B1	2005-07-26	Spyker, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	20	6931379	B1	2005-08-16	Sato, et al.	
	21	7546956	B2	2009-06-16	Adams, et al.	
	22	7793355	B2	2010-09-07	Little, et al.	
	23	7815100	B2	2010-10-19	Adams, et al.	
	24	8302185	B2	2012-10-30	Little, et al.	
	25	8429410	B2	2013-04-23	Little, et al.	
	26	8887988	B2	2014-11-18	Adams, et al.	
	27	9033216	B2	2015-05-19	Adams, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010002485	A1	2001-05-31	Bisbee, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	2	20010032188	A1	2001-10-18	Miyabe, et al.	
	3	20020007454	A1	2002-01-17	Tarpenning, et al.	
	4	20020152376	A1	2002-10-17	Eigeles	
	5	20030172034	A1	2003-09-11	Schneck, et al.	
	6	20030191719	A1	2003-10-09	Ginter, et al.	
	7	20040039911	A1	2004-02-26	Oka, et al.	
	8	20040078565	A1	2004-22-04	Hofmeister, et al.	
	9	20050050319	A1	2005-03-03	Suraski	
	10	20060272028	A1	2006-11-30	Maes	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	1	0384610	EP	A2	1992-02-06	International Business Machines		☐
	2	2312767	GB	A	1997-11-05	Mitel Corporation		☐
	3	0828209	EP	A2	1998-03-11	Samsung Electronics, Ltd.		☐
	4	1998044404	WO	A1	1998-10-08	Sun Mircrosystems, Inc.		☐
	5	0060434	WO	A1	2000-10-12	Microsoft Corporation		☐
	6	2355819	GB	A	2001-05-02	Marconi Communications United		☐
	7	2001171590	WO	A1	2001-09-27	Vasara Research, Inc.		☐
	8	2001077811	WO	A1	2001-10-18	Everdream, Inc.		☐
	9	1168141	EP	A2	2002-01-02	Franklin Electronic Publishers, Inc.		☐
	10	2002056360	JP	A	2002-02-20	Hitachi, Ltd.		☒
	11	2002091598	JP	A	2002-03-29	Nippon Computer Co., Ltd.		☒

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	12	2002170063	JP	A	2002-06-14	NTT Communications		☒
	13	2002182963	JP	A	2002-06-28	Ricoh Co., Ltd.		☒
	14	2002097620	WO	A2	2002-12-05	Qualcomm Incorporated		☐
	15	2825565	FR	A1	2002-12-06	Sagem		☒
	16	2378780	GB	A	2003-02-19	Elan Digital Systems Limited		☐
	17	2333865	GB	B	2003-05-14	International Business Machines Corp.		☐
	18	2003058411	WO	A1	2003-07-17	NTT Docomo, Inc.		☐
	19	2003063524	WO	A1	2003-07-31	Yahoo, Inc.		☐
	20	1185923	EP	B1	2004-03-31	Elata Limited		☐
	21	1427166	EP	A2	2004-06-09	Canon Kabushiki Kaisha		☐
	22	1465041	EP	A2	2004-10-06	NTT Docomo, Inc.		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	23	0813132	EP	B1	2005-01-26	International Business Machines Corporation		☐
	24	2429148	EP	A2	2012-03-14	NTT DoCoMo, Inc.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	TAKARAGI; "Angou Houshiki to Ouyou [Encryption system and Application]"; Journal of Information Processing; Volume 32, No. 6; Japan: Information Processing Society of Japan; June 1991; 11 pages. (as referenced in Japanese Office Action dated February 10, 2009 for Application No. 2004-557718)	☐
	2	BOS, BERT; "Re: CSS: Extended Tiling. Proposal"; www-style@w3.org, http://lists.w3.org/Archives/Public/www-style/2004May/0020.html; May 5, 2004; 2 pages.	☐
	3	W3C; "CSS3 Module: Border"; http://www.w3.org/TR/2002/WD-css3-border-20021107/ November 7, 2002; 14 pages.	☐
	4	W3C; "CSS3 Backgrounds and Borders Module"; www.w3.org/TR/2005/WD-css3-background-20050216/; February 16, 2005; 30 pages.	☐
	5	SAMARATI, Pierangela, et al.; "Access Control: Policies, Models, and Mechanisms"; Foundations of Security Analysis and Design; Lecture Notes in Computer Science Volume 2171; 2001; 60 pages.	☐
	6	Microsoft; "Managing Authorization and Access Control"; http://technet.microsoft.com/en-us/library/bb457115.aspx; November 3, 2005; 84 pages.	☐
	7	CLARKSON, Michael; "Access Control"; http://www.cs.cornell.edu/courses/cs513/2007fa/NL.accessControl.html; 2007; 8 pages.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	8	Wikipedia; "Access Control List"; http://en.wikipedia.org/wiki/Access_control_list; retrieved July 2, 2013; 3 pages.	☐
	9	Wikipedia; "Access Control List"; http://en.wikipedia.org/wiki/Access_control_list; retrieved June 5, 2013; 1 page.	☐
	10	Office Action dated August 21, 2007; U.S. Application No. 10/784,024 filed February 20, 2004; 21 pages. 10802-US-PAT	☐
	11	Office Action dated June 11, 2007; U.S. Application No. 10/732,132 filed December 10, 2003; 13 pages. (4214-27101)	☐
	12	Office Action dated February 22, 2008; U.S. Application No. 10/732,132 filed December 10, 2003; 11 pages. (4214-27101)	☐
	13	Final Office Action dated September 23, 2008; U.S. Application No. 10/732,132 filed December 10, 2003; 9 pages. (4214-27101)	☐
	14	Advisory Action dated December 8, 2008; U.S. Application No. 10/732,132 filed December 10, 2003; 3 pages. (4214-27101)	☐
	15	Office Action dated April 2, 2009; U.S. Application No. 10/732,132 filed December 10, 2003; 10 pages. (4214-27101)	☐
	16	Final Office Action dated October 28, 2009; U.S. Application No. 10/732,132 filed December 10, 2003; 10 pages. (4214-27101)	☐
	17	Advisory Action dated January 19, 2010; U.S. Application No. 10/732,132 filed December 10, 2003; 3 pages. (4214-27101)	☐
	18	Notice of Allowance dated May 4, 2010; U.S. Application No. 10/732,132 filed December 10, 2003; 7 pages. (4214-27101)	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	19	Office Action dated August 3, 2011; U.S. Application No. 12/869,589 filed August 26, 2010; 20 pages. (4214-27115)	☐
	20	Office Action dated January 19, 2012; U.S. Application No. 12/869,589 filed August 26, 2010; 11 pages. (4214-27115)	☐
	21	Notice of Allowance dated June 13, 2012; U.S. Application No. 12/869,589 filed August 26, 2010; 9 pages. (4214-27115)	☐
	22	Office Action dated June 17, 2013; U.S. Application No. 13/606,814 filed September 7, 2012; 19 pages. (4214-27116)	☐
	23	Final Office Action dated October 10, 2013; U.S. Application No. 13/606,814 filed September 7, 2012; 6 pages. (4214-27116)	☐
	24	Office Action dated May 29, 2008; U.S. Application No. 11/118,844 filed April 29, 2005; 4 pages. (4214-25701)	☐
	25	Office Action dated March 10, 2009; U.S. Application No. 11/118,844 filed April 29, 2005; 6 pages. (4214-25701)	☐
	26	Office Action dated August 20, 2009; U.S. Application No. 11/118,844 filed April 29, 2005; 15 pages. (4214-25701)	☐
	27	Notice of Allowance dated February 23, 2010; U.S. Application No. 11/118,844 filed April 29, 2005; 7 pages. (4214-25701)	☐
	28	Notice of Allowance dated June 10, 2010; U.S. Application No. 11/118,844 filed April 29, 2005; 8 pages. (4214-25701)	☐
	29	Office Action dated April 7, 2008; U.S. Application No. 11/118,748 filed April 29, 2005; 11 pages. (4214-25702)	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	30	Final Office Action dated October 27, 2008; U.S. Application No. 11/118,748 filed April 29, 2005; 10 pages. (4214-25702)	☐
	31	Notice of Allowance dated February 9, 2009; U.S. Application No. 11/118,748 filed April 29, 2005; 6 pages. (4214-25702)	☐
	32	Office Action dated March 22, 2010; U.S. Application No. 12/468,441 filed May 19, 2009; 12 pages. (4214-25703)	☐
	33	Notice of Allowance dated August 11, 2010; U.S. Application No. 12/468,441 filed May 19, 2009; 12 pages. (4214-25703)	☐
	34	Office Action dated November 12, 2013; U.S. Application No. 12/885,281 filed September 17, 2010; 32 pages. (4214-25712)	☐
	35	Office Action dated April 3, 2014; U.S. Application No. 12/885,281 filed September 17, 2010; 9 pages. (4214-25712)	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DANIEL HESS/	Date Considered	06/27/2015

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2015-06-04
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown /DANIEL HESS/
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	1	PCT International Search Report; Application No. PCT/CA2004/000250; September 14, 2004; 3 pages. (10802-WO-PCT)	☐
	2	PCT Written Opinion of the International Searching Authority; Application No. PCT/CA2004/000250; September 14, 2004; 6 pages. (10802-WO-PCT)	☐
	3	European Examination Report; Application No. 04712985.3; December 22, 2006; 5 pages. (10802-EP-EPT)	☐
	4	PCT International Search Report; Application No. PCT/CA2003/01944; July 12, 2004; 6 pages. (4214-27102)	☐
	5	Australian Office Action; Application No. 2003292922; May 10, 2007; 2 pages. (4214-27103)	☐
	6	Canadian Office Action; Application No. 2,509,358; May 8, 2008; 2 pages. (4214-27105)	☐
	7	Canadian Office Action; Application No. 2,509,358; November 20, 2009; 2 pages. (4214-27105)	☐
	8	Canadian Office Action; Application No. 2,509,358; November 25, 2010; 2 pages. (4214-27105)	☐
	9	Canadian Notice of Allowance; Application No. 2,509,358; November 14, 2011; 1 page. (4214-27105)	☐
	10	Chinese Office Action; Application No. 200380109662.2; February 2, 2007; 7 pages. (4214-27106)	☒
	11	Chinese Office Action; Application No. 200380109662.2; January 18, 2008; 5 pages. (4214-27106)	☒

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	12	Chinese Office Action; Application No. 200380109662.2; August 21, 2009; 6 pages. (4214-27106)	☒
	13	European Examination Report; Application No. 03788723.9; September 10, 2007; 7 pages. (4214-27107)	☐
	14	European Summons to Attend Oral Proceedings; Application No. 03788723.9; June 29, 2010; 11 pages. (4214-27107)	☐
	15	Indian Office Action; Application No. 2481/DELNP/2005; April 12, 2007; 2 pages. (4214-27109)	☐
	16	Indian Office Action; Application No. 3101/DELNP/2008; September 30, 2013; 1 page. (4214-27110)	☐
	17	Japanese Office Action; Application No. 2004-557718; February 10, 2009; 12 pages. (4214-27111)	☒
	18	Japanese Office Action; Application No. 2004-557718; March 9, 2010; 8 pages. (4214-27111)	☒
	19	Korean Office Action; Application No. 10-2005-7010726; September 29, 2006; 9 pages. (4214-27113)	☒
	20	PCT International Search Report; Application No. PCT/CA2005/000650; August 22, 2005; 3 pages. (4214-25704)	☐
	21	PCT Written Opinion of the International Searching Authority; Application No. PCT/CA2005/000650; August 22, 2005; 7 pages. (4214-25704)	☐
	22	PCT International Search Report; Application No. PCT/CA2005/000653; August 25, 2005; 5 pages. (4214-25705)	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	23	PCT Written Opinion of the International Searching Authority; Application No. PCT/CA2005/000653; August 25, 2005; 7 pages. (4214-25705)	☐
	24	Canadian Office Action; Application No. 2,564,186; June 26, 2009; 2 pages. (4214-25706)	☐
	25	Canadian Office Action; Application No. 2,564,186; August 6, 2010; 2 pages. (4214-25706)	☐
	26	Canadian Office Action; Application No. 2,564,186; August 30, 2011; 2 pages. (4214-25706)	☐
	27	Canadian Office Action; Application No. 2,564,186; October 18, 2012; 2 pages. (4214-25706)	☐
	28	Canadian Office Action; Application No. 2,564,186; February 11, 2014; 2 pages. (4214-25706)	☐
	29	Canadian Office Action; Application No. 2,564,186; March 17, 2015; 4 pages. (4214-25706)	☐
	30	Canadian Office Action; Application No. 2,564,285; February 13, 2009; 3 pages. (4214-25707)	☐
	31	Canadian Office Action; Application No. 2,564,285; August 4, 2011; 3 pages. (4214-25707)	☐
	32	Canadian Office Action; Application No. 2,564,285; August 14, 2012; 3 pages. (4214-25707)	☐
	33	European Search Report; Application No. 05739066.8; July 23, 2007; 3 pages. (4214-25708)	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	34	European Examination Report; Application No. 05739066.8; December 17, 2007; 5 pages. (4214-25708)	☐
	35	European Examination Report; Application No. 05739066.8; February 17, 2010; 5 pages. (4214-25708)	☐
	36	European Invitation Pursuant to Article 94(3) and Rule 71(1) EPC; Application No. 05739066.8; May 20, 2011; 4 pages. (4214-25708)	☐
	37	European Search Report; Application No. 05741262.9; September 26, 2007; 11 pages. (4214-25709)	☐
	38	European Examination Report; Application No. 05741262.9; February 20, 2008; 4 pages. (4214-25709)	☐
	39	European Examination Report; Application No. 05741262.9; May 3, 2010; 9 pages. (4214-25709)	☐
	40	Notice of Allowance dated July 16, 2014; U.S. Application No. 12/885,281 filed September 17, 2010; 12 pages. (4214-25712)	☐
	41	Office Action dated January 17, 2013; U.S. Application No. 13/618,311 filed September 14, 2012; 17 pages. (4214-25713)	☐
	42	Office Action dated June 28, 2013; U.S. Application No. 13/618,311 filed September 14, 2012; 10 pages. (4214-25713)	☐
	43	Final Office Action dated October 30, 2013; U.S. Application No. 13/618,311 filed September 14, 2012; 9 pages. (4214-25713)	☐
	44	Advisory Action dated January 3, 2014; U.S. Application No. 13/618,311 filed September 14, 2012; 3 pages. (4214-25713)	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	45	Office Action dated April 2, 2014; U.S. Application No. 13/618,311 filed September 14, 2012; 9 pages. (4214-25713)	☐
	46	Notice of Allowance dated July 10, 2014; U.S. Application No. 13/618,311 filed September 14, 2012; 20 pages. (4214-25713)	☐
	47	Notice of Allowance dated January 7, 2015; U.S. Application No. 13/618,311 filed September 14, 2012; 9 pages. (4214-25713)	☐
	48	Notice of Allowance dated October 23, 2013; Application No. 13/561,374 filed July 30, 2012; 5 pages. (21344-US-CNT2)	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DANIEL HESS/	Date Considered	06/27/2015

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2015-06-04
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown /DANIEL HESS/
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5560008		1996-09-24	Johnson, et al.	
	2	5619710		1997-04-08	Travis, Jr., et al.	
	3	5778348		1998-07-07	Manduley, et al.	
	4	5944821		1999-08-31	Angelo	
	5	6061794		2000-05-09	Angelo, et al.	
	6	6101607		2000-08-08	Bachand, et al.	
	7	6134659		2000-10-17	Sprong, et al.	
	8	6134593		2000-10-17	Alexander, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	9	6141754		2000-10-31	Choy	
	10	6167521		2000-12-26	Smith, et al.	
	11	6192476	B1	2001-02-20	Gong	
	12	6202207	B1	2011-03-13	Donohue	
	13	6212635	B1	2001-04-03	Reardon	
	14	6216116	B1	2001-04-10	Barkan, et al.	
	15	6233608	B1	2001-05-15	Laursen, et al.	
	16	6480961	B2	2002-11-12	Rajasekharan, et al.	
	17	6487665	B1	2002-11-26	Andrew, et al.	
	18	6513121	B1	2003-01-28	Serkowski	
	19	6922782	B1	2005-07-26	Spyker, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	20	6931379	B1	2005-08-16	Sato, et al.	
	21	7546956	B2	2009-06-16	Adams, et al.	
	22	7793355	B2	2010-09-07	Little, et al.	
	23	7815100	B2	2010-10-19	Adams, et al.	
	24	8302185	B2	2012-10-30	Little, et al.	
	25	8429410	B2	2013-04-23	Little, et al.	
	26	8887988	B2	2014-11-18	Adams, et al.	
	27	9033216	B2	2015-05-19	Adams, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010002485	A1	2001-05-31	Bisbee, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	2	20010032188	A1	2001-10-18	Miyabe, et al.	
	3	20020007454	A1	2002-01-17	Tarpenning, et al.	
	4	20020152376	A1	2002-10-17	Eigeles	
	5	20030172034	A1	2003-09-11	Schneck, et al.	
	6	20030191719	A1	2003-10-09	Ginter, et al.	
	7	20040039911	A1	2004-02-26	Oka, et al.	
	8	20040078565	A1	2004-22-04	Hofmeister, et al.	
	9	20050050319	A1	2005-03-03	Suraski	
	10	20060272028	A1	2006-11-30	Maes	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	1	0384610	EP	A2	1992-02-06	International Business Machines		☐
	2	2312767	GB	A	1997-11-05	Mitel Corporation		☐
	3	0828209	EP	A2	1998-03-11	Samsung Electronics, Ltd.		☐
	4	1998044404	WO	A1	1998-10-08	Sun Mircrosystems, Inc.		☐
	5	0060434	WO	A1	2000-10-12	Microsoft Corporation		☐
	6	2355819	GB	A	2001-05-02	Marconi Communications United		☐
	7	2001171590	WO	A1	2001-09-27	Vasara Research, Inc.		☐
	8	2001077811	WO	A1	2001-10-18	Everdream, Inc.		☐
	9	1168141	EP	A2	2002-01-02	Franklin Electronic Publishers, Inc.		☐
	10	2002056360	JP	A	2002-02-20	Hitachi, Ltd.		☒
	11	2002091598	JP	A	2002-03-29	Nippon Computer Co., Ltd.		☒

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	12	2002170063	JP	A	2002-06-14	NTT Communications		☒
	13	2002182963	JP	A	2002-06-28	Ricoh Co., Ltd.		☒
	14	2002097620	WO	A2	2002-12-05	Qualcomm Incorporated		☐
	15	2825565	FR	A1	2002-12-06	Sagem		☒
	16	2378780	GB	A	2003-02-19	Elan Digital Systems Limited		☐
	17	2333865	GB	B	2003-05-14	International Business Machines Corp.		☐
	18	2003058411	WO	A1	2003-07-17	NTT Docomo, Inc.		☐
	19	2003063524	WO	A1	2003-07-31	Yahoo, Inc.		☐
	20	1185923	EP	B1	2004-03-31	Elata Limited		☐
	21	1427166	EP	A2	2004-06-09	Canon Kabushiki Kaisha		☐
	22	1465041	EP	A2	2004-10-06	NTT Docomo, Inc.		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	23	0813132	EP	B1	2005-01-26	International Business Machines Corporation		☐
	24	2429148	EP	A2	2012-03-14	NTT DoCoMo, Inc.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	TAKARAGI; "Angou Houshiki to Ouyou [Encryption system and Application]"; Journal of Information Processing; Volume 32, No. 6; Japan: Information Processing Society of Japan; June 1991; 11 pages. (as referenced in Japanese Office Action dated February 10, 2009 for Application No. 2004-557718)	☐
	2	BOS, BERT; "Re: CSS: Extended Tiling. Proposal"; www-style@w3.org, http://lists.w3.org/Archives/Public/www-style/2004May/0020.html; May 5, 2004; 2 pages.	☐
	3	W3C; "CSS3 Module: Border"; http://www.w3.org/TR/2002/WD-css3-border-20021107/ November 7, 2002; 14 pages.	☐
	4	W3C; "CSS3 Backgrounds and Borders Module"; www.w3.org/TR/2005/WD-css3-background-20050216/; February 16, 2005; 30 pages.	☐
	5	SAMARATI, Pierangela, et al.; "Access Control: Policies, Models, and Mechanisms"; Foundations of Security Analysis and Design; Lecture Notes in Computer Science Volume 2171; 2001; 60 pages.	☐
	6	Microsoft; "Managing Authorization and Access Control"; http://technet.microsoft.com/en-us/library/bb457115.aspx; November 3, 2005; 84 pages.	☐
	7	CLARKSON, Michael; "Access Control"; http://www.cs.cornell.edu/courses/cs513/2007fa/NL.accessControl.html; 2007; 8 pages.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	8	Wikipedia; "Access Control List"; http://en.wikipedia.org/wiki/Access_control_list; retrieved July 2, 2013; 3 pages.	☐
	9	Wikipedia; "Access Control List"; http://en.wikipedia.org/wiki/Access_control_list; retrieved June 5, 2013; 1 page.	☐
	10	Office Action dated August 21, 2007; U.S. Application No. 10/784,024 filed February 20, 2004; 21 pages. 10802-US-PAT	☐
	11	Office Action dated June 11, 2007; U.S. Application No. 10/732,132 filed December 10, 2003; 13 pages. (4214-27101)	☐
	12	Office Action dated February 22, 2008; U.S. Application No. 10/732,132 filed December 10, 2003; 11 pages. (4214-27101)	☐
	13	Final Office Action dated September 23, 2008; U.S. Application No. 10/732,132 filed December 10, 2003; 9 pages. (4214-27101)	☐
	14	Advisory Action dated December 8, 2008; U.S. Application No. 10/732,132 filed December 10, 2003; 3 pages. (4214-27101)	☐
	15	Office Action dated April 2, 2009; U.S. Application No. 10/732,132 filed December 10, 2003; 10 pages. (4214-27101)	☐
	16	Final Office Action dated October 28, 2009; U.S. Application No. 10/732,132 filed December 10, 2003; 10 pages. (4214-27101)	☐
	17	Advisory Action dated January 19, 2010; U.S. Application No. 10/732,132 filed December 10, 2003; 3 pages. (4214-27101)	☐
	18	Notice of Allowance dated May 4, 2010; U.S. Application No. 10/732,132 filed December 10, 2003; 7 pages. (4214-27101)	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	19	Office Action dated August 3, 2011; U.S. Application No. 12/869,589 filed August 26, 2010; 20 pages. (4214-27115)	☐
	20	Office Action dated January 19, 2012; U.S. Application No. 12/869,589 filed August 26, 2010; 11 pages. (4214-27115)	☐
	21	Notice of Allowance dated June 13, 2012; U.S. Application No. 12/869,589 filed August 26, 2010; 9 pages. (4214-27115)	☐
	22	Office Action dated June 17, 2013; U.S. Application No. 13/606,814 filed September 7, 2012; 19 pages. (4214-27116)	☐
	23	Final Office Action dated October 10, 2013; U.S. Application No. 13/606,814 filed September 7, 2012; 6 pages. (4214-27116)	☐
	24	Office Action dated May 29, 2008; U.S. Application No. 11/118,844 filed April 29, 2005; 4 pages. (4214-25701)	☐
	25	Office Action dated March 10, 2009; U.S. Application No. 11/118,844 filed April 29, 2005; 6 pages. (4214-25701)	☐
	26	Office Action dated August 20, 2009; U.S. Application No. 11/118,844 filed April 29, 2005; 15 pages. (4214-25701)	☐
	27	Notice of Allowance dated February 23, 2010; U.S. Application No. 11/118,844 filed April 29, 2005; 7 pages. (4214-25701)	☐
	28	Notice of Allowance dated June 10, 2010; U.S. Application No. 11/118,844 filed April 29, 2005; 8 pages. (4214-25701)	☐
	29	Office Action dated April 7, 2008; U.S. Application No. 11/118,748 filed April 29, 2005; 11 pages. (4214-25702)	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

	30	Final Office Action dated October 27, 2008; U.S. Application No. 11/118,748 filed April 29, 2005; 10 pages. (4214-25702)	☐
	31	Notice of Allowance dated February 9, 2009; U.S. Application No. 11/118,748 filed April 29, 2005; 6 pages. (4214-25702)	☐
	32	Office Action dated March 22, 2010; U.S. Application No. 12/468,441 filed May 19, 2009; 12 pages. (4214-25703)	☐
	33	Notice of Allowance dated August 11, 2010; U.S. Application No. 12/468,441 filed May 19, 2009; 12 pages. (4214-25703)	☐
	34	Office Action dated November 12, 2013; U.S. Application No. 12/885,281 filed September 17, 2010; 32 pages. (4214-25712)	☐
	35	Office Action dated April 3, 2014; U.S. Application No. 12/885,281 filed September 17, 2010; 9 pages. (4214-25712)	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/DANIEL HESS/	Date Considered	06/27/2015

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2015-06-04
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DH/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/715,227	05/18/2015	Neil P. Adams	11913-US-CNT3 4214-25714	5874

82313 7590 07/08/2015

Conley Rose - BlackBerry Files
Attn: J. Robert Brown
5601 Granite Parkway, Suite 500
Plano, TX 75024

EXAMINER	
HESS, DANIEL A	

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
07/08/2015	ELECTRONIC

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

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

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

ConleyRoseReporting@dfw.conleyrose.com

Office Action Summary	Application No. 14/715,227	Applicant(s) ADAMS ET AL.	
	Examiner DANIEL HESS	Art Unit 2876	AIA (First Inventor to File) Status No

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

Period for Reply

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

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

Status

1)☒ Responsive to communication(s) filed on *5/18/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

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

Disposition of Claims*

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

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

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

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

Application Papers

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

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

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *6/4/2015*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

This action is responsive to 5/18/2015 filing by applicant.

The present application is being examined under the pre-AIA first to invent provisions.

Claim Rejections - 35 USC § 102

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

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-5, 9, 10, 12-16 and 20 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Fisher et al. (US 2003/0101292).

Re claim 1:

Fisher applies to an electronic device.

Fisher teachs at para [0004]:

"**In order to permit multiple users to access a single computer system, the various users (and their applications) are assigned various separate resources within the system.** For instance, **various memory addresses are assigned to one user application** and various other memory addresses are assigned to another to avoid overlap. This is known in the art as sandboxing. Such separation is used to avoid interference between applications that can

cause undesired effects to occur."

Fisher teaches at para [0006]:

"**Substantially all multiprogrammed systems rely upon software and/or hardware solutions that prevent applications from accessing memory addresses that are out of the permissible range.** The software solutions typically at least statically review the instructions of a particular application when it is loaded to determine whether any of the instructions contain a direct memory reference to an out-of-range memory address."

Fisher shows the principle whereby multiple users on a computer system and the applications associated with that user are granted access to certain local memory and barred access to other local memory. This achieves several ends as the above excerpt demonstrates:

(1) Memory can be allocated to users and their applications can only use the memory that belongs to their owners.

(2) A first application cannot access and interfere with the memory of a second different application, possibly by a different user.

In keeping with the above, application identifiers would be associated with user identifiers and memory is associated with user identifiers. Users of a system in turn would have their own authorizations to be able to access the system and applications gain authorization to access certain memory through those users.

It is noted that this principle of delineated memory seen above applies both on a larger level to user accounts and on a finer level to multiple applications belonging to the same user.

Re claims 2 and 3: Memory access by an application as described above generally includes all of read, write and erase ability.

Re claims 4 and 5: The relation between an owner and memory use for specific applications has been seen above.

"Insertion of additional owner information" would be restricted at least in the sense that another user on the same level could not on their own obtain access to memory and applications belonging to a different user. That is the meaning of assigning users control.

Re claims 9 and 10: Fisher clearly can apply (as seen in the excerpt above) to user accounts that may have multiple applications in them. The authorization record, which is associated with one user, applies to two or more applications.

Re claims 12-16: See discussions re claims 1-4, above.

Re claim 20: See discussion re claim 1 above.

Claim Rejections - 35 USC § 103

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

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

Claims 6-8, 11 and 17-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over by Fisher et al.

Re claim 6: See para 0039, where it is seen that the system in question can be a server computer. Server computers are conventionally accessed remotely for both control and providing service to clients. Wireless networks could reasonably be part of the remote access configuration in Fisher et al.

Re claims 7 and 8: Claims 1 and 7 to a good approximation describe the configuration that has been present at the USPTO since prior to the instant invention. An external server system managed by the USPTO administers all policies. Specifically the server supplies users with access to applications and pushes applications for users. Users have specifically allocated memory on servers for their accounts and to be used by their application.

This is similar to what is seen in paragraphs 0004 and 0006 of Fisher, but with organizational control.

Re claim 11: In the case of organization controlled IT, described above, regular users may not install or delete any application within their allocated space. This an administrative-level function. Users certainly can run applications and operate within applications to create and delete data files associated with those applications, but they may not control the installation and authorizations of applications. This is a protected data store.

Re claims 17-19: See discussion re claims 6-8, above.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Bishop et al. (US 5,784,552) and Kisliakov (US 2003/0178482) and McGrath (US 2004/0210760) all teach memory allocations that are 'sandboxed' for different applications.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANIEL HESS whose telephone number is (571)272-2392. The examiner can normally be reached on 9:00 AM - 5:00 PM M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/DANIEL HESS/
Primary Examiner, Art Unit 2876

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14715227	ADAMS ET AL.
	Examiner	Art Unit
	DANIEL HESS	2876

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	375, 380	6/27/2015	DH
719	328		

SEARCH NOTES		
Search Notes	Date	Examiner
East keyword searches attached	6/27/2015	DH

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	23	(prohibit$4 near2 application near4 access$5 near2 memory)	US-PGPUB; USPAT	OR	ON	2015/06/27 09:48
L3	169	(memory near1 access$4) with application with (authoriz$6 or permission)	US-PGPUB; USPAT	OR	ON	2015/06/27 09:58
L4	6	((memory near1 access$4) with application with (authoriz$6 or permission)).ab.	US-PGPUB; USPAT	OR	ON	2015/06/27 09:58
L5	7	3 and (owner near2 information)	US-PGPUB; USPAT	OR	ON	2015/06/27 10:04
L6	29	3 and owner	US-PGPUB; USPAT	OR	ON	2015/06/27 10:04
L7	1	"20030101292".did.	US-PGPUB; USPAT	OR	ON	2015/06/27 11:08

EAST Search History (Interference)

<This search history is empty>

6/27/2015 12:53:06 PM

Nintendo Exhibit 1003
Part 1 of 2
Page 00370

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14715227
	Filing Date	2015-05-18
	First Named Inventor	Neil P. Adams
	Art Unit	2143
	Examiner Name	Unknown
	Attorney Docket Number	11913-US-CNT3 4214-25714

	1	PCT International Search Report; Application No. PCT/CA2004/000250; September 14, 2004; 3 pages. (10802-WO-PCT)	☐
	2	PCT Written Opinion of the International Searching Authority; Application No. PCT/CA2004/000250; September 14, 2004; 6 pages. (10802-WO-PCT)	☐
	3	European Examination Report; Application No. 04712985.3; December 22, 2006; 5 pages. (10802-EP-EPT)	☐
	4	PCT International Search Report; Application No. PCT/CA2003/01944; July 12, 2004; 6 pages. (4214-27102)	☐
	5	Australian Office Action; Application No. 2003292922; May 10, 2007; 2 pages. (4214-27103)	☐
	6	Canadian Office Action; Application No. 2,509,358; May 8, 2008; 2 pages. (4214-27105)	☐
	7	Canadian Office Action; Application No. 2,509,358; November 20, 2009; 2 pages. (4214-27105)	☐
	8	Canadian Office Action; Application No. 2,509,358; November 25, 2010; 2 pages. (4214-27105)	☐
	9	Canadian Notice of Allowance; Application No. 2,509,358; November 14, 2011; 1 page. (4214-27105)	☐
	10	Chinese Office Action; Application No. 200380109662.2; February 2, 2007; 7 pages. (4214-27106)	☒
	11	Chinese Office Action; Application No. 200380109662.2; January 18, 2008; 5 pages. (4214-27106)	☒

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14715227
	Filing Date	2015-05-18
	First Named Inventor	Neil P. Adams
	Art Unit	2143
	Examiner Name	Unknown
	Attorney Docket Number	11913-US-CNT3 4214-25714

	12	Chinese Office Action; Application No. 200380109662.2; August 21, 2009; 6 pages. (4214-27106)	☒
	13	European Examination Report; Application No. 03788723.9; September 10, 2007; 7 pages. (4214-27107)	☐
	14	European Summons to Attend Oral Proceedings; Application No. 03788723.9; June 29, 2010; 11 pages. (4214-27107)	☐
	15	Indian Office Action; Application No. 2481/DELNP/2005; April 12, 2007; 2 pages. (4214-27109)	☐
	16	Indian Office Action; Application No. 3101/DELNP/2008; September 30, 2013; 1 page. (4214-27110)	☐
	17	Japanese Office Action; Application No. 2004-557718; February 10, 2009; 12 pages. (4214-27111)	☒
	18	Japanese Office Action; Application No. 2004-557718; March 9, 2010; 8 pages. (4214-27111)	☒
	19	Korean Office Action; Application No. 10-2005-7010726; September 29, 2006; 9 pages. (4214-27113)	☒
	20	PCT International Search Report; Application No. PCT/CA2005/000650; August 22, 2005; 3 pages. (4214-25704)	☐
	21	PCT Written Opinion of the International Searching Authority; Application No. PCT/CA2005/000650; August 22, 2005; 7 pages. (4214-25704)	☐
	22	PCT International Search Report; Application No. PCT/CA2005/000653; August 25, 2005; 5 pages. (4214-25705)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14715227
	Filing Date	2015-05-18
	First Named Inventor	Neil P. Adams
	Art Unit	2143
	Examiner Name	Unknown
	Attorney Docket Number	11913-US-CNT3 4214-25714

	23	PCT Written Opinion of the International Searching Authority; Application No. PCT/CA2005/000653; August 25, 2005; 7 pages. (4214-25705)	☐
	24	Canadian Office Action; Application No. 2,564,186; June 26, 2009; 2 pages. (4214-25706)	☐
	25	Canadian Office Action; Application No. 2,564,186; August 6, 2010; 2 pages. (4214-25706)	☐
	26	Canadian Office Action; Application No. 2,564,186; August 30, 2011; 2 pages. (4214-25706)	☐
	27	Canadian Office Action; Application No. 2,564,186; October 18, 2012; 2 pages. (4214-25706)	☐
	28	Canadian Office Action; Application No. 2,564,186; February 11, 2014; 2 pages. (4214-25706)	☐
	29	Canadian Office Action; Application No. 2,564,186; March 17, 2015; 4 pages. (4214-25706)	☐
	30	Canadian Office Action; Application No. 2,564,285; February 13, 2009; 3 pages. (4214-25707)	☐
	31	Canadian Office Action; Application No. 2,564,285; August 4, 2011; 3 pages. (4214-25707)	☐
	32	Canadian Office Action; Application No. 2,564,285; August 14, 2012; 3 pages. (4214-25707)	☐
	33	European Search Report; Application No. 05739066.8; July 23, 2007; 3 pages. (4214-25708)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14715227
	Filing Date	2015-05-18
	First Named Inventor	Neil P. Adams
	Art Unit	2143
	Examiner Name	Unknown
	Attorney Docket Number	11913-US-CNT3 4214-25714

	34	European Examination Report; Application No. 05739066.8; December 17, 2007; 5 pages. (4214-25708)	☐
	35	European Examination Report; Application No. 05739066.8; February 17, 2010; 5 pages. (4214-25708)	☐
	36	European Invitation Pursuant to Article 94(3) and Rule 71(1) EPC; Application No. 05739066.8; May 20, 2011; 4 pages. (4214-25708)	☐
	37	European Search Report; Application No. 05741262.9; September 26, 2007; 11 pages. (4214-25709)	☐
	38	European Examination Report; Application No. 05741262.9; February 20, 2008; 4 pages. (4214-25709)	☐
	39	European Examination Report; Application No. 05741262.9; May 3, 2010; 9 pages. (4214-25709)	☐
	40	Notice of Allowance dated July 16, 2014; U.S. Application No. 12/885,281 filed September 17, 2010; 12 pages. (4214-25712)	☐
	41	Office Action dated January 17, 2013; U.S. Application No. 13/618,311 filed September 14, 2012; 17 pages. (4214-25713)	☐
	42	Office Action dated June 28, 2013; U.S. Application No. 13/618,311 filed September 14, 2012; 10 pages. (4214-25713)	☐
	43	Final Office Action dated October 30, 2013; U.S. Application No. 13/618,311 filed September 14, 2012; 9 pages. (4214-25713)	☐
	44	Advisory Action dated January 3, 2014; U.S. Application No. 13/618,311 filed September 14, 2012; 3 pages. (4214-25713)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14715227
	Filing Date	2015-05-18
	First Named Inventor	Neil P. Adams
	Art Unit	2143
	Examiner Name	Unknown
	Attorney Docket Number	11913-US-CNT3 4214-25714

	45	Office Action dated April 2, 2014; U.S. Application No. 13/618,311 filed September 14, 2012; 9 pages. (4214-25713)	☐
	46	Notice of Allowance dated July 10, 2014; U.S. Application No. 13/618,311 filed September 14, 2012; 20 pages. (4214-25713)	☐
	47	Notice of Allowance dated January 7, 2015; U.S. Application No. 13/618,311 filed September 14, 2012; 9 pages. (4214-25713)	☐
	48	Notice of Allowance dated October 23, 2013; Application No. 13/561,374 filed July 30, 2012; 5 pages. (21344-US-CNT2)	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14715227
Filing Date	2015-05-18
First Named Inventor	Neil P. Adams
Art Unit	2143
Examiner Name	Unknown
Attorney Docket Number	11913-US-CNT3 4214-25714

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/J. Robert Brown, Jr./	Date (YYYY-MM-DD)	2015-06-04
Name/Print	J. Robert Brown, Jr.	Registration Number	45438

This collection of information is required by 37 CFR 1.97 and 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 1 hour 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.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION

(PCT Rule 44.1)

To:
BORDEN LADNER GERVAIS LLP
Attn. Wong, Jeffrey W.
1100-100 Queen Street
Ottawa, Ontario K1P 1J9
CANADA

Date of mailing *(day/month/year)* 12/07/2004	
Applicant's or agent's file reference PAT 55929W-90	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/CA 03/01944	International filing date *(day/month/year)* 12/12/2003

Applicant

RESEARCH IN MOTION LIMITED

1. [x] The applicant is hereby notified that the International Search Report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the International Search Report; however, for more details, see the notes on the accompanying sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Fascimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no International Search Report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. [ ] **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

[ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

[ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

Within **19 months** from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within **20 months** from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Jacinta Reddy

Form PCT/ISA/220 (July 1998)

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the PCT Applicant's Guide, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

BNSDOCID <XS ISA220NOENP4 1 >

Nintendo Exhibit 1003
Part 1 of 2
Page 00380

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped),whether

(i) the claim is unchanged;

(ii) the claim is cancelled;

(iii) the claim is new;

(iv) the claim replaces one or more claims as filed;

(v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."

2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."

3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."

4. [Where various kinds of amendments are made]:
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international appplication is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the same time of filing the amendments with the International Bureau, also file a copy of such amendments with the International Preliminary Examining Authority (see Rule 62.2(a), first sentence).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, where upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see Volume II of the PCT Applicant's Guide.

BNSDOCID <XS ISA220NOENP4 1 >

Nintendo Exhibit 1003
Part 1 of 2
Page 00381

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference PAT 55929W-90	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/CA 03 01944	International filing date *(day/month/year)* 12/12/2003	(Earliest) Priority Date *(day/month/year)* 12/12/2002
Applicant RESEARCH IN MOTION LIMITED		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 6

   [X] as suggested by the applicant.

   [ ] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [ ] None of the figures.

Nintendo Exhibit 1003
Part 1 of 2
Page 00382

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 03/01944

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 061 794 A (DRISCOLL DAN J ET AL) 9 May 2000 (2000-05-09) column 4, line 54 - line 67	26
A	EP 1 168 141 A (FRANKLIN ELECTRONIC PUBLISHERS) 2 January 2002 (2002-01-02) the whole document	1-25, 27-30
A	EP 0 828 209 A (SAMSUNG ELECTRONICS CO LTD) 11 March 1998 (1998-03-11) the whole document	20
A	US 5 944 821 A (ANGELO MICHAEL F) 31 August 1999 (1999-08-31) the whole document	1-25, 27-30

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 July 2004	12/07/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax. (+31-70) 340-3016	Meis, M

2

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 03/01944

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6061794 A	09-05-2000	NONE	
EP 1168141 A	02-01-2002	EP 1168141 A2	02-01-2002
		US 2001056533 A1	27-12-2001
EP 0828209 A	11-03-1998	KR 232400 B1	01-12-1999
		EP 0828209 A2	11-03-1998
		JP 10133762 A	22-05-1998
		TW 399182 B	21-07-2000
		US 5978920 A	02-11-1999
US 5944821 A	31-08-1999	NONE	

Form PCT/ISA/210 (patent family annex) (January 2004)

COPY

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
BORDEN LADNER GERVAIS LLP
World Exchange Plaza
1100 - 100 Queen Street
OTTAWA, Ontario
Canada, K1P 1J9

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)* 25 August 2005 (25-08-2005)

Applicant's or agent's file reference
PAT 59031W-90

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/CA2005/000653	29 April 2005 (29-04-2005)	30 April 2004 (30-04-2004)

International Patent Classification (IPC) or both national classification and IPC
IPC(7): G06F 9/445, H04Q 7/38, H04Q 7/32, H04L 12/22, G06F 12/14

Applicant
RESEARCH IN MOTION LIMITED

1. This opinion contains indications relating to the following items :

[X]	Box No. I	Basis of the opinion
[ ]	Box No. II	Priority
[ ]	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
[X]	Box No. IV	Lack of unity of invention
[X]	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(I) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
[ ]	Box No. VI	Certain documents cited
[ ]	Box No. VII	Certain defects in the international application
[X]	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**
If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later. (Nov 25/05)
(Feb 28/06) - entered gco
For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/CA	Date of completion of this opinion	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	22 August 2005 (22-08-2005)	Cristian S. Popa (819) 997-2299

Nintendo Exhibit 1003
Part 1 of 2
Page 00385

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   [X] the international application in the language in which it was filed

   [ ] a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material

      [ ] a sequence listing

      [ ] table(s) related to the sequence listing

   b. format of material

      [ ] on paper

      [ ] in electronic form

   c. time of filing/furnishing

      [ ] contained in the international application as filed.

      [ ] filed together with the international application in electronic form

      [ ] furnished subsequently to this Authority for the purposes of search.

3 [ ] In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statement that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments :

Nintendo Exhibit 1003
Part 1 of 2
Page 00386

Box No. IV **Lack of unity of invention**

1. [ ] In response to the invitation (Form PCT/ISA/206) to pay additional fees the applicant has, within the applicable time limit :

   [ ] paid additional fees

   [ ] paid additional fees under protest and, where applicable, the protest fee

   [ ] paid additional fees under protest but the applicable protest fee was not paid

   [X] not paid additional fees

2. [ ] This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

   [ ] complied with

   [X] not complied with for the following reasons :

   1. Claims 1-22, 30 and 31*: Owner application control of an electronic device based upon a list of applications required for the device to be fully operational*

   2. Claims 23-29: *Owner application control of an electronic device by authorizing a user request to install an application based upon an application identifier and owner control information*

   3. Claims 32- 42: *Owner control of operations on an electronic device based upon authorizing the execution of one or more operations associated with a particular application*

4. Consequently, this opinion has been established in respect of the following parts of the international application :

   [ ] all parts

   [X] the parts relating to claim Nos. 1-22, 30 and 31

Nintendo Exhibit 1003
Part 1 of 2
Page 00387

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(I) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-19, 21, 22 , 30, 31	YES
	Claims	20	NO
Inventive step (IS)	Claims	none	YES
	Claims	1-22 , 30, 31	NO
Industrial applicability (IA)	Claims	1-22, 30, 31	YES
	Claims		NO

2. Citations and explanations :

Reference is made to the following documents:

D1: EP 1185923 B1
D2: WO 03/063524 A1
D3: US 20010032188 A1

1. In relation to claim 1, 18, 19 and 30, D1 teaches a method of content control for an electronic device, the method comprising:
- verifying ([0091]: *"compares a profile"*) that an application ([0091]: *"automatic distribution, installation ... including applications"*; claim 13) listed in a required list ([0012]: *"distribution of certain core content to devices"*; [0041]: *"profile of content (for example programs and data) that are desired by the network authority to be present on the device"*; [0091]: *"profile generated by the server"*) is available for execution on the device;
- if the application in the required list is not verified as available ([0091]: *"any new and updated content"*), initiating download and installation of the application of the application from an external application source ([0091]: *"automatically retrieved and installed"*).
D1 does not teach the disabling at least one operation of the device untill the application on the required list is available for execution on the device.
However, D2 teaches the disabling of operations of an electronic device when a corresponding application is not available for execution on the device (page 33 lines 18-20: *"features are disabled ... if ... the client .. cannot support the feature"*; claims 26, 28).
In relation to claims 15 and 31, the recitation of these claims extends the disabling step until all unavailable applications are becoming available for execution on the electronic device. One skilled in the art would have arrived without an inventive efort to the teachings of claim 15 and 31 having regard to D1 and in view of the disablement of unsupported features described in D2.
Claims 1, 15, 18, 19 and 30 lack an inventive step in view of D1 and D2 (see **7.** for rejection of claim 31).

2. In relation to claim 2, D1 teaches receiving the required list from an external list source ([0008]: *"a server ... to generate profile for the device"*; Fig1B).
Claim 2 lacks an inventive step in view of D1 and D2.

3. In relation to claim 3, D1 teaches receiving an update to the required list from the external list source and updating the required list based on upon the received update ([0023]: "it will automatically receive an updated profile").
Even though D1 does not explicitly teach the alternative of *receiving the update from a second external source* as in claim 3, it should be noted that such a feature could be either inferred directly from D1 or relate to normal parctices and procedures known to a person skilled in the art.
Claim 3 lacks an inventive step in view of D1 and D2.

4. In relation to claim 4, D1 teaches receiving an update of the required list from a server (col. 23 lines 36-38) and receiving applications also from servers acting as *external application sources* (claim 4).
Even though D1 does not explicitly teach the alternative of using *the external application source* as *enxternal list source*, D1 teaches both of these sources as being servers. Thus, one skilled in the art would have arrived without an inventive activity to the teachings of claim 4 in view of D1 and D2.
Claim 4 lacks an inventive step in view of D1 and D2.

Continued in Supplemental Box ...

Nintendo Exhibit 1003
Part 1 of 2
Page 00388

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made :

The description is objected to under PCT Rule 5.1(a) (ii) because no relevant background art disclose was not included in description..

Claims 7 to 10, 16, 19, 20 and 21 are objected to under PCT Article 6 because these claims are indefinite for the following reasons:

- in claim 1 the language *"disabling at least one operation of the device"* requires elaboration because it is not clear if the *operation* corresponds to the application verified as not available or is chosen based upon a different criterion;
- claims 7 to 10 are ambiguous because of the following contradiction: an application listed in a *required list* (claim 1 line 5) could be absent from the *allowed list* (claim 7 lines 30, 31), in other words an application required for the device to be fully operational is may not be allowed;
- in claim 7, where the *allowed list* is stored remains unspecified;
- in claim 11, where in the system the *receiving an application installation request* takes place and where the request originates remains unspecified;
- in claim 16 where the *receiving an operation request* takes place and where the *request* originates remains unspecified;
- in claim 16, the location where *the authorization record* is stored remains unspecified;
- signal claim 19 fails to specify the tangible character of the supporting medium, e.g. *"computer data signal embodied in a carrier wave comprising computer code means for:"*;
- in claims 20 and 21 where exactly in the system the *receiving* and *determining* steps take place remains unspecified;
- in claim 21 line 6, the term *the electronic device* is ambiguous because of antecedent recitation of *a first electronic device* and *a second electronic device.*

Nintendo Exhibit 1003
Part 1 of 2
Page 00389

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of: **Box No. V**

5. In relation to claim 5, D1 teaches receiving and updating the required list prior to verification step (col. 23 lines 29-45).
Claim 5 lacks an inventive step in view of D1 and D2.

6. In relation to claim 6, D1 teaches requesting the update from the external source (claim 12: *"to request the profile"*).
Even though D1 does not explicitly teach the alternative of *requesting the update from a second external source* as in claim 6, it should be noted that such a feature could be either inferred directly from D1 or relate to normal parctices and procedures known to a person skilled in the art.
Claim 6 lacks an inventive step in view of D1 and D2.

7. In relation to claims 7 to 9 and 31, D3 teaches the installation of only the applications present on an *allowed list* ([0145]: *"installation approved"*and Fig. 10), wherein the allowed information is received from an external information source (abstract, [0145]) and wherein receiving an update of the *allowed list* from the external list source (Figs. 15, 16, [0171]: *"updated distribution information", "updated data base"*).
In relation to claim 10, neither D1 nor D3 teach explicitely the updating of the *required* list based upon the received update to the *allowed* list. However, such a feature is described inherently by D1 and D3 because if any of the applications on the the required list are not also allowed application, the claimed embodiment could not operate at all untill such update takes place.
Claims 7 to 10 and 31 lack an inventive step in view of D1 and D2 and D3.

8. In relation to claim 11, D3 further teaches receiving an application installation request, and initiating installation after an approval response is received from an external computer system to which to-be installed application identification information was previously sent (see abstract, claim 33, [0145]: *"installation approved"*).
In relation to claim 12, D1 teaches an external computer providing the *application source* to the electronic device (claim 2: *"location from which that content can be obtained"*).
Including the *application source* described in D1 with the *approval response* described in D3 is a design choice which could be either inferred directly from D1 in view of D3 or relate to normal practices and procedures known to a person skilled in the art.
In relation to claim 13, D1 teaches dowloading the to-be installed application from the application source([0087]: *"content is downloaded from the location indicated ... "*).
In relation to claim 14, D3 teaches consulting an *excluded list* based on the tansmited identification information and transmitting a *denial* or an *approval* response, based on the presence or respectively the absence of the *to-be installed application* on the *excluded list* ([0141], [0145], [0146]: *"program looks up the installation property", "installation approved", "installation disapproved"* and Fig. 10).
Claims 11 to 14 lack an inventive step in view of D1 and D2 and D3.

9. In relation to claims 16, D3 teaches:
-receiving an operation request from an application ([0016]; [0138]-[0146] and Fig. 6 item S602);
-determining whether the requested operation is allowed to be performed by the application based upon a stored authorization ([0141]: *"the installation propriety ... recorded as data for each serial number")* and an application identifier (Fig. 6 item S613: "SERIAL NUMBER") associated with the application;
-allowing the application to perform the requested operation only if the requested operation is determined to be allowed to be performed by the application ([0144]-[0146]: *"installation program waits for receiving the response information", "installation approved", "installation disapproved"* and Fig 6 items S615- S618).
In relation to claim 17, even though D1 , D2 and D3 do not describe specifically the features presented in these claims, it should be noted that these features relate to normal practices and procedures known to a person skilled in the art.
Claims 16 and 17 lack an inventive step in view of D1 and D2 and D3.

10. In relation to claim 20 , D1 teaches:
-receiving a required list request (claim 12: *"request the profile"*) from a first electronic device for a list of one or more applications required by the owner of the electronic device for full operation of the device ([0041]: *"profile of content (for example programs and data) that are desired by the network authority to be present on the device")*, wherein the required list request comprises an identifier associated with the electronic device ([0041]: *"communicates the identity of the device to a server "*);
-determining the required list based upon the identifier in the received required list request ([0041]: *"server which replies with a profile of content"*); and
-transmitting the determined required list to the first electronic device ([0041]: *"the server transmits ... the location from which ... can be retrieved"*).
Claim 20 lacks novelty over D1.

11. In relation to claims 21, D1 teaches:
-receiving a list request (claim 12) from a first electronic device for one or more applications (claim 13) , wherein the list request
Continued in Supplemental Box ...

Nintendo Exhibit 1003
Part 1 of 2
Page 00390

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of: **Box No. V**

comprises an identifier associated with the electronic device([0041] *"communicates the identity of the device to a server"*);
-determining the required list based upon the identifier in the received required list request ([0041]: *"server which. replies with a profile of content"*); and
-transmitting the determined list to the first electronic device ([0041]: *"the server transmits ... the location from which ... can be retrieved"*).
D3 teaches installing of only the applications present on an *allowed list* ([0145]: *installation approved"* and Fig. 10).
In relation to claim 22, D1 teaches the electronic devices as being wireless mobile communication devices ([0007], Fig. 1C items 110).
Claims 21 and 22 lack an inventive step in view of D1 and D3.

Claims 1 to 6, 15, 18, 19 and 30 appear to lack an inventive step under PCT Article 33(3) as being obvious in view of documents D1 and D2.

Claims 7 to 14, 16, 17 and 31 appear to lack an inventive step under PCT Article 33(3) as being obvious in view of documents D1 and D2 and D3.

Claims 20 appears to lack novelty under PCT Article 33(2) in view of document D1.

Claims 21 and 22 appear to lack an inventive step under PCT Article 33(3) as being obvious in view of documents D1 and D3.

The claimed subject matter of claims 1-22, 30 and 31 is considered to be industrially applicable under article 33(4) PCT.

Nintendo Exhibit 1003
Part 1 of 2
Page 00391

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
PAT 56260W-90		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/CA2004/000250	20/02/2004	21/02/2003
Applicant		
RESEARCH IN MOTION LIMITED		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
      [ ] The international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box II).

3. [ ] **Unity of invention is lacking** (see Box III).

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant.
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant.
   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regards to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 4
      [X] as suggested by the applicant.
      [ ] as selected by this Authority, because the applicant failed to suggest a figure.
      [ ] as selected by this Authority, because this figure better characterizes the invention.
   b. [ ] none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA2004/000250

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 378 780 A (ELAN DIGITAL SYSTEMS LTD) 19 February 2003 (2003-02-19) the whole document	1-26
A	EP 1 168 141 A (FRANKLIN ELECTRONIC PUBLISHERS) 2 January 2002 (2002-01-02) the whole document	1-26
A	WO 00/60434 A (MICROSOFT CORP) 12 October 2000 (2000-10-12) the whole document	1-26

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 July 2004	14/09/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Meis, M

7

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA2004/000250

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
GB 2378780	A	19-02-2003	WO	03017069 A2	27-02-2003
EP 1168141	A	02-01-2002	EP	1168141 A2	02-01-2002
			US	2001056533 A1	27-12-2001
WO 0060434	A	12-10-2000	AU	4068100 A	23-10-2000
			WO	0060434 A1	12-10-2000

COPY **PATENT COOPERATION TREATY**

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/CA2004/000250	20.02.2004	21.02.2003

International Patent Classification (IPC) or both national classification and IPC
G06F1/00

Applicant
RESEARCH IN MOTION LIMITED

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☒ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

(Dec 14/04)

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

(Dec 21/04)

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Entered gco

Name and mailing address of the ISA:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer

Meis, M

Telephone No. +49 89 2399-2505

Form PCT/ISA/237 (Cover Sheet) (January 2004)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was field, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ in written format

   ☐ in computer readable form

   c. time of filing/furnishing:

   ☐ contained in the international application as filed.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Nintendo Exhibit 1003
Part 1 of 2
Page 00396

Box No. II Priority

1. ☒ The following document has not been furnished:

   ☒ copy of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(a)).

   ☐ translation of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(b)).

   Consequently it has not been possible to consider the validity of the priority claim. This opinion has nevertheless been established on the assumption that the relevant date is the claimed priority date.

2. ☐ This opinion has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rules 43*bis*.1 and 64.1). Thus for the purposes of this opinion, the international filing date indicated above is considered to be the relevant date.

3. Additional observations, if necessary:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-26
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-26
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-26
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Nintendo Exhibit 1003
Part 1 of 2
Page 00397

SECTION V

1. The following documents are referred to in this communication:

   D1 : GB 2 378 780 A (ELAN DIGITAL SYSTEMS LTD) 19 February 2003 (2003-02-19)
   D2 : EP 1 168 141 A (FRANKLIN ELECTRONIC PUBLISHERS) 2 January 2002 (2002-01-02)
   D3 : WO 00/60434 A (MICROSOFT CORP) 12 October 2000 (2000-10-12)

   Document D1 pertains to access pay-by-use software by consuming tokens obtained by network.

   Document D2 pertains to restricting use of application programs and object files on a secure computer platform based on the application programs and object files being provided with a correctly signed hash.

   Document D3, pertains to restrict access to applications on a user level based on application category information and control information in a database. The database may be updated by network.

2. (a) The subject-matter of independent claim 1 differs from the disclosure of documents D1, D2 and D3 in that the authorisation information (D1: token; D2: signed application programmer's public signature key (par. 38); D3: database information) is received for a selected authorisation level and is stored in association with the selected authorisation level.

   The subject-matter of claim 1 is therefore novel (Article 33(2) PCT).

   (c) The problem to be solved by the present invention may be regarded as: provide a multiple-level control of the device rather than a single level control of the device.

   (c) The solution to this problem proposed in claim 1 of the present application is considered as involving an inventive step (Article 33(3) PCT) for the following reasons:
   Neither the problem, nor the solution are mentioned in any of the documents

cited in the search report.

3. Claims 2-14 are dependent on claim 1 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

4. Claim 15 comprises all the features of claim 1 and, as such, also meets the requirements of the PCT with respect to novelty and inventive step.

5. Claim 16 comprises all the features of claim 1 (the controlled information corresponding to authorisation information) and as such also meet the requirements of the PCT with respect to novelty and inventive step.

6. Claim 17 is dependent on claim 16 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

7. Claim 18 comprises all the features of claim 1 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

8. (a) The subject-matter of independent claim 19 essentially differs from the disclosure of document D1, (i) in that the authorisation information (token) is stored for each of a plurality of authorisation levels, (ii) in that each controlled information is associated with an authorisation level and (iii) in that no authorisation information may be required to perform the requested operation (use of pay-by-use software). (The controlled information is embodied in D1 by the information stored in the token record file additional to the tokens.)

(b) The subject-matter of independent claim 19 essentially differs from the disclosure of document D2 in the above features (i), (ii) and (iii) (wherein the authorisation information corresponds to the signed application programmer's public signature key in D2) and (iv) in that no controlled information is provided.

The subject-matter of independent claim 19 essentially differs from the disclosure of D3 in the above features (i), (ii), (iii).

Documents D1 and D2, thus represents the most relevant state of the art.

The subject-matter of claim 19 is therefore novel (Article 33(2) PCT)

(c) The problem to be solved by the present invention with respect to the most relevant prior art may be regarded as:
provide a multiple-level control of the device rather than a single level control of the device (features (i) and (ii)) and less restrictions regarding allowing performance of requested operations (feature (iii)).

(d) The solution to this problem proposed in claim 19 of the present application is considered as involving an inventive step (Article 33(3) PCT) for the following reasons:
Neither the problems, nor the solution are mentioned in any of the documents cited in the search report.

9. Claims 20-16 are dependent on claim 19 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

10. The claimed subject-matter is industrially applicable.

SECTION VIII

1. It is not clear (Art. 6 PCT) in cl. 10, 16 and 19 what is implied by "controlled" information. It has been assumed that authorisation information is meant.

2. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

–

Electronic Acknowledgement Receipt

EFS ID:	22541794
Application Number:	14715227
International Application Number:	
Confirmation Number:	5874
Title of Invention:	System and Method of Owner Application Control of Electronic Devices
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	82313
Filer:	J. Robert Brown/Rami Law
Filer Authorized By:	J. Robert Brown
Attorney Docket Number:	11913-US-CNT3 4214-25714
Receipt Date:	04-JUN-2015
Filing Date:	18-MAY-2015
Time Stamp:	17:05:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	11913-US-CNT3_2015-06-04_IDS1_b.pdf	616170 76c86d637a94ecc34c3dc042e978019f702018b9	no	8

Warnings:	
Information:	

A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.

2	Other Reference-Patent/App/Search documents	10802-WO-PCT_2004-09-14_PCTSearch.pdf	332753 a05217e42c12769b5641d4790918f7cd29656a52	no	3
Warnings:					
Information:					
3	Other Reference-Patent/App/Search documents	10802-WO-PCT_2004-09-14_PCTOpinion.pdf	720919 7aa994909f9094fe45cbee9d9dc3478d23438006	no	6
Warnings:					
Information:					
4	Other Reference-Patent/App/Search documents	10802-EP-EPT_2006-12-22_EPExam.pdf	557771 286c31549e34c62bb84ad5606f42b7942afc96e6	no	5
Warnings:					
Information:					
5	Other Reference-Patent/App/Search documents	PCTSearch_27102_071204.pdf	812998 764de299652a342edc649f5448bd72f3b43f2cfb	no	6
Warnings:					
Information:					
6	Other Reference-Patent/App/Search documents	AUOfficeAction_27103_051007.pdf	113517 8e15a043df9cf2464006389a93ac30d39c2ad69f	no	2
Warnings:					
Information:					
7	Other Reference-Patent/App/Search documents	CAOfficeAction_27105_050808.pdf	141221 af2a87343cc742c05a67971825eaa865940d3615	no	2
Warnings:					
Information:					
8	Other Reference-Patent/App/Search documents	CAOfficeAction_27105_112009.pdf	167655 ee63d324fdaaba9b0a1eacdca96f13538ba633cf	no	2
Warnings:					
Information:					
9	Other Reference-Patent/App/Search documents	CAOfficeAction_27105_112510.pdf	274850 9458050d077a53b062c410d8530bf8765158e1dd	no	2
Warnings:					
Information:					

10	Other Reference-Patent/App/Search documents	CAAllowance_27105_111411.pdf	273926 0be4b8021cca01fb4acd180baf826cf73101549a	no	1
Warnings:					
Information:					
11	Other Reference-Patent/App/Search documents	CNOfficeAction_27106_020207.pdf	244230 a4ef2617387a1089067be6ad8448ddbb6c060c23	no	7
Warnings:					
Information:					
12	Other Reference-Patent/App/Search documents	CNOfficeAction_27106_011808.pdf	178548 86f906dfa0a391564eef60b2b639fb823088559d	no	5
Warnings:					
Information:					
13	Other Reference-Patent/App/Search documents	CNOfficeAction_27106_082109.pdf	225181 0aa07242982452aeaf85932a77dd5ad51e15f5c8	no	6
Warnings:					
Information:					
14	Other Reference-Patent/App/Search documents	EPExam_27107_091007.pdf	914736 0560affa2a6cf8b7ba69d0af1dd1ead4879d905b	no	7
Warnings:					
Information:					
15	Other Reference-Patent/App/Search documents	EPSummons_27107_062910.pdf	1759856 b29e21e8215f468e453b84e295ebaa53d1e2782c	no	11
Warnings:					
Information:					
16	Other Reference-Patent/App/Search documents	INOfficeAction_27109_041207.pdf	213776 7cfad38e163d38694a5933f04607aeb80d254054	no	2
Warnings:					
Information:					
17	Other Reference-Patent/App/Search documents	INOfficeAction_27110_093013.pdf	219253 d9cb8c8be5e7442fdce448624a42b2650e73bc2a	no	1
Warnings:					
Information:					
18	Other Reference-Patent/App/Search documents	JPOfficeAction_27111_021009.pdf	1450016 b7c028f5cd10010bd2e24914f36cb910e4033efa	no	12
Warnings:					
Information:					

19	Other Reference-Patent/App/Search documents	JPOfficeAction_27111_030910.pdf	955457 95fae403c5f4eedc85cc7d0cad340ee2321944f9	no	8
Warnings:					
Information:					
20	Other Reference-Patent/App/Search documents	KROfficeAction_27113_092906.pdf	1691013 f05625acfe0b5b7371367503cf1d543b7aeb7b60	no	9
Warnings:					
Information:					
21	Other Reference-Patent/App/Search documents	PCTSearch_25704_082205.pdf	153872 2729d6a92c796d50f2b410b3c42dc01fbdd6caba	no	3
Warnings:					
Information:					
22	Other Reference-Patent/App/Search documents	PCTOpinion_25704_082205.pdf	346768 4bde82781ffd9bd488ea84a683a0ad371471b4bb	no	7
Warnings:					
Information:					
23	Other Reference-Patent/App/Search documents	PCTSearch_25705_082505.pdf	255385 c3d05f8b797acc63b24ba4aa3481721d71651421	no	5
Warnings:					
Information:					
24	Other Reference-Patent/App/Search documents	PCTOpinion_25705_082505.pdf	374327 763dbdde2cf66f0fda18dea1b240d193a3a95619	no	7
Warnings:					
Information:					
25	Other Reference-Patent/App/Search documents	CAOfficeAction_25706_062609.pdf	163766 29c02b4261c53c3e30105ff25484e4b0d71467b3	no	2
Warnings:					
Information:					
26	Other Reference-Patent/App/Search documents	CAOfficeAction_25706_080610.pdf	278950 ad57270f710b116226225c98a4fc84122cb34542	no	2
Warnings:					
Information:					
27	Other Reference-Patent/App/Search documents	CAOfficeAction_25706_083011.pdf	192560 b9cb18ea8b97af2e49cd0b02042b7599844d3502	no	2
Warnings:					
Information:					

28	Other Reference-Patent/App/Search documents	CAOfficeAction_25706_101812.PDF	168233 42f663af4b30984c959cc3006f2bd2668027980a	no	2
Warnings:					
Information:					
29	Other Reference-Patent/App/Search documents	CAOfficeAction_25706_021114.pdf	168557 542a1a9ed001672810b7f6d3fe33b1296d530d99	no	2
Warnings:					
Information:					
30	Other Reference-Patent/App/Search documents	CAOfficeAction_25706_031715.pdf	345614 b71864b7091c67610b3d3dac5634457cce358857	no	4
Warnings:					
Information:					
31	Other Reference-Patent/App/Search documents	CAOfficeAction_25707_021309.pdf	198828 324976f9237952bf8cd90787e809a7df04378c58	no	3
Warnings:					
Information:					
32	Other Reference-Patent/App/Search documents	CAOfficeAction_25707_080411.pdf	206811 e584bb6daedd4aa01cee1c742645dcab893d27f4	no	3
Warnings:					
Information:					
33	Other Reference-Patent/App/Search documents	CAOfficeAction_25707_081412.pdf	218090 a64b123c933979eeb9e95061a30a427eb5b163c0	no	3
Warnings:					
Information:					
34	Other Reference-Patent/App/Search documents	EPSearch_25708_072307.pdf	208325 d72a58b0f3e93cc42c285115c9f15a80136722ee	no	3
Warnings:					
Information:					
35	Other Reference-Patent/App/Search documents	EPExam_25708_121707.pdf	352831 4038b0e90700475a4e30c318bf4fd9d2c73d3bf6	no	5
Warnings:					
Information:					
36	Other Reference-Patent/App/Search documents	EPExam_25708_021710.pdf	376842 cff4b236f9da6a62683c3b2f81cd2f7d47f889af	no	5
Warnings:					
Information:					

37	Other Reference-Patent/App/Search documents	EPInvitation_25708_052011.pdf	196069 91f38c6705efac1fa1be1dce07afbc57ca41a0d7	no	4
Warnings:					
Information:					
38	Other Reference-Patent/App/Search documents	EPExam_25709_050310.pdf	996120 3469c519cf18821f62fb578b3ba43d0359035a2f	no	9
Warnings:					
Information:					
39	Other Reference-Patent/App/Search documents	EPExam_25709_022008.pdf	262151 ff4c4b179f3fdc7260b1c3d1c9a5619cd058210d	no	4
Warnings:					
Information:					
40	Other Reference-Patent/App/Search documents	NOA_25712_071614.pdf	603571 f3c995da8903708e4e8d525b29542a20b3b5c39b	no	12
Warnings:					
Information:					
41	Other Reference-Patent/App/Search documents	OA_25713_011713.pdf	566446 f1e877963bcef288f7f1ca65af9cdfa7c4446474	no	17
Warnings:					
Information:					
42	Other Reference-Patent/App/Search documents	OA_25713_062813.pdf	351149 81172df39105c8c4b8fc3c24eebb72e24bc41b39	no	10
Warnings:					
Information:					
43	Other Reference-Patent/App/Search documents	FOA_25713_103013.pdf	330302 1501259a2dc107f8577c6e7d1e6b9a3ab2b8935d	no	9
Warnings:					
Information:					
44	Other Reference-Patent/App/Search documents	AA_25713_010314.pdf	137192 db10662467e7fadab89de2a6c6bcb553cd2a2c0a	no	3
Warnings:					
Information:					
45	Other Reference-Patent/App/Search documents	OA_25713_040214.pdf	289686 50d046bf7778bcacdf88c706b65357697e2cf5d6	no	9
Warnings:					
Information:					

46	Other Reference-Patent/App/Search documents	NOA_25713_071014.pdf	896437 5475634450346e7f31882d3dabca99428244a926	no	20
Warnings:					
Information:					
47	Other Reference-Patent/App/Search documents	NOA_25713_010715.pdf	1175497 d3f39574a154428a9bc6ed79bdcad12c518aac23	no	9
Warnings:					
Information:					
48	Other Reference-Patent/App/Search documents	21344-US-CNT2_NOA_102313.pdf	669625 c7d31770ad1679dc00316d62870fc47e52ce4fa6	no	5
Warnings:					
Information:					
49	Other Reference-Patent/App/Search documents	EPSearch_25709_092607.pdf	1228670 9ae8f371534f31d82f26a101d867609f24ce3884	no	11
Warnings:					
Information:					
		Total Files Size (in bytes):	23576520		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PATENT COOPERATION TREATY

PCT

COPY

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference PAT 59031W-90	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below
International application No. **PCT/CA2005/000653**	International filing date *(day/month/year)* 29 April 2005 (29-04-2005)	(Earliest)Priority date *(day/month/year)* 30 April 2004 (30-04-2004)
Applicant RESEARCH IN MOTION LIMITED		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 5 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of:

      [X] the international application in the language in which it was filed

      [ ] a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

   b. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I

2. [ ] **Certain claims were found unsearchable** (see Box No. II)

3. [X] **Unity of invention is lacking** (see Box No. III)

4. With regard to the **title**,

   [X] the text is approved as submitted by the applicant

   [ ] the text has been established by this Authority to read as follows :

5. With regard to the **abstract**,

   [X] the text is approved as submitted by the applicant

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,

   a. the figure of the **drawings** to be published with the abstract is Figure No. 2

      [X] as suggested by the applicant

      [ ] as selected by this Authority, because the applicant failed to suggest a figure

      [ ] as selected by this Authority, because this figure better characterizes the invention

   b. [ ] none of the figures is to be published with the abstract

Nintendo Exhibit 1003
Part 1 of 2
Page 00408

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of the first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons :

1. [ ] Claim Nos. :
because they relate to subject matter not required to be searched by this Authority, namely :

2. [ ] Claim Nos. :
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically :

3. [ ] Claim Nos. :
because they are dependant claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows :

1. Claims 1-22, 30 and 31: *Owner application control of an electronic device based upon a list of applications required for the device to be fully operational*
2. Claims 23-29: *Owner application control of an electronic device by authorizing a user request to install an application based upon an application identifier and owner control information*
3. Claims 32- 42: *Owner control of operations on an electronic device based upon authorizing the execution of one or more operations associated with a particular application*

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claim Nos. :

4. [X] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim Nos. : 1-22, 30 and 31

Remark on Protest
[ ] The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
[ ] The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
[ ] No protest accompanied the payment of additional search fees.

Nintendo Exhibit 1003
Part 1 of 2
Page 00409

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/000653

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7): G06F 9/445, H04Q 7/38, H04Q 7/32, H04L 12/22, G06F 12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(7): G06F, H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Delphion, Canadian Patent Database, IEEE Xplore, & keywords: owner control, application, electronic device, installation, download, required list, disable operation /execution, user access, content control, authentication, authorization, permission, restriction, excluded, allowed, denied

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1185923 B1 (*Jackson et al*) 31 March 2004 (31-03-2004) [0041], claim 12	20
Y	[0007], [0008], [0021], [0023], [0041], [0087], [0091], col. 23 lines 29-45, claims 2, 4, 12, 13, Fig. 1B	1-19, 21, 22, 30, 31
Y	WO 03063524 A1 (*Tzan-En Szeto et al.*) 31 July 2003 (31-07-2003) page 33 lines 18-20, claims 26, 28	1-19
Y	US 20010032188 A1 (*Miyabe et al.*) 18 Oct. 2001 (18-10-2001) [0016], [0138]-[0146], [0171] and Figs. 1C, 6, 10, 15, 16	7-14, 16, 17 , 21, 22, 30, 31
A	US 20030191719 A1 (*Ginter et al.*) 9 Oct. 2003 (09-10-2003) - the whole document -	1-42

[ ] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 July 2005 (06-07-2005)	25 August 2005 (25-08-2005)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Cristian S. Popa (819) 997-2299

Nintendo Exhibit 1003
Part 1 of 2
Page 00410

EP1185923	31-03-2004	AT263392T T	15-04-2004
		AU4132900 A	17-11-2000
		DE60009489D D1	06-05-2004
		DE60009489T T2	23-12-2004
		EP1185923 A2	13-03-2002
		ES2215638T T3	16-10-2004
		GB2352539 A	31-01-2001
		GB9910164D D0	30-06-1999
		GB9922348D D0	24-11-1999
		HK1033990 A1	25-06-2004
		IL145993D D0	25-07-2002
		JP2002543515T T	17-12-2002
		US6886017 B1	26-04-2005
		WO0067112 A2	09-11-2000
WO03063524	31-07-2003	EP1468576 A1	20-10-2004
		US2003140103 A1	24-07-2003
		WO03063524 A1	31-07-2003
US2001032188	18-10-2001	JP2001312439 A	09-11-2001
		US2001032188 A1	18-10-2001
US2003191719	09-10-2003	AU711733 B2	21-10-1999
		AU739300 B2	11-10-2001
		AU739693 B2	18-10-2001
		AU756500 B2	16-01-2003
		AU3205797 A	05-12-1997
		AU3681597 A	19-02-1998
		AU3681697 A	19-02-1998
		AU3684097 A	19-02-1998
		AU4170397 A	19-03-1998
		AU6326696 A	18-09-1996
		AU7106296 A	26-03-1998
		CA2212574 A1	06-09-1996
		CA2264819 A1	12-03-1998
		CA2265473 A1	05-03-1998
		CA2373508 A1	05-03-1998
		CA2373542 C	12-11-2002
		CA2480118 A1	05-03-1998
		CN1139067C C	18-02-2004
		CN1183841 A	03-06-1998
		CN1492429 A	28-04-2004
		CN1577205 A	09-02-2005
		EP0861461 A2	02-09-1998
		EP0898777 A2	03-03-1999
		EP0922248 A1	16-06-1999
		EP0974129 A1	26-01-2000
		EP1431864 A2	23-06-2004
		EP1515216 A2	16-03-2005
		EP1526472 A2	27-04-2005
		EP1531379 A2	18-05-2005
		JP10512074T T	17-11-1998
		JP2000516743T T	12-12-2000
		JP2001501763T T	06-02-2001
		JP2004005558 A	08-01-2004
		JP2004005601 A	08-01-2004
		JP2004005614 A	08-01-2004
		JP2004005625 A	08-01-2004
		JP2004005629 A	08-01-2004
		JP2004030600 A	29-01-2004
		JP2004139550 A	13-05-2004
		JP2004265358 A	24-09-2004
		US5892900 A	06-04-1999
		US5910987 A	08-06-1999
		US5915019 A	22-06-1999
		US5917912 A	29-06-1999

Nintendo Exhibit 1003
Part 1 of 2
Page 00411

US5943422 A	24-08-1999		
		US5949876 A	07-09-1999
		US5982891 A	09-11-1999
		US6157721 A	05-12-2000
		US6185683 B1	06-02-2001
		US6237786 B1	29-05-2001
		US6240185 B1	29-05-2001
		US6253193 B1	26-06-2001
		US6292569 B1	18-09-2001
		US6363488 B1	26-03-2002
		US6389402 B1	14-05-2002
		US6427140 B1	30-07-2002
		US6449367 B2	10-09-2002
		US6618484 B2	09-09-2003
		US6640304 B2	28-10-2003
		US6658568 B1	02-12-2003
		US2001042043 A1	15-11-2001
		US2002023214 A1	21-02-2002
		US2002048369 A1	25-04-2002
		US2002112171 A1	15-08-2002
		US2003041239 A1	27-02-2003
		US2003105721 A1	05-06-2003
		US2003163431 A1	28-08-2003
		US2003191719 A1	09-10-2003
		US2004054630 A1	18-03-2004
		US2004103305 A1	27-05-2004
		US2004123129 A1	24-06-2004
		US2004133793 A1	08-07-2004
		US2005060584 A1	17-03-2005
		WO9627155 A2	06-09-1996
		WO9743761 A2	20-11-1997
		WO9809209 A1	05-03-1998
		WO9810381 A1	12-03-1998
		CN 1601429A	30-03-2005

Nintendo Exhibit 1003
Part 1 of 2
Page 00412

COPY

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference PAT 59029W-90	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below
International application No. **PCT/CA2005/000650**	International filing date *(day/month/year)* 29 April 2005 (29-04-2005)	(Earliest)Priority date *(day/month/year)* 30 April 2004 (30-04-2004)
Applicant RESEARCH IN MOTION LIMITED ET AL		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of:

      [X] the international application in the language in which it was filed

      [ ] a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

   b. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I

2. [ ] **Certain claims were found unsearchable** (see Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No. III)

4. With regard to the **title**,

   [X] the text is approved as submitted by the applicant

   [ ] the text has been established by this Authority to read as follows :

5. With regard to the **abstract**,

   [X] the text is approved as submitted by the applicant

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,

   a. the figure of the **drawings** to be published with the abstract is Figure No. 2

      [X] as suggested by the applicant

      [ ] as selected by this Authority, because the applicant failed to suggest a figure

      [ ] as selected by this Authority, because this figure better characterizes the invention

   b. [ ] none of the figures is to be published with the abstract

Nintendo Exhibit 1003
Part 1 of 2
Page 00413

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/000650

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7): G06F 12/14, H04Q 7/32, H04L 9/32, H04M 1/67

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(7): G06F, H04Q 7/32, H04L 9/32, H04M 1/67

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Delphion, Pluspat, Canadian Patent Database (application, control, request, operation, identifier, authorization, permission, corporate, organization, policies, devices, records)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/77811 A1 Jooste 18 October 2001 (18-10-2001) *see whole document	1-18
X	WO 03058411 A1 Yamada et al. 17 July 2003 (17-07-2003)	1-7, 9-18
A	*see whole document	8
X,P	EP 1465041 A2 Ichikawa et al. 6 October 2004 (06-10-2004)	1-7, 9-18
A,P	*see whole document	8
X	US 6513121 B1 Serkowski 28 January 2003 (28-01-2003)	1, 2, 9-12, 14-17
A	*see whole document	3-6, 13, 18
A, P	US 2005/0050319 A1 Suraski 3 March 2005 (03-03-2005) *abstract, paragraph [0009]	1-4, 6, 10, 11, 13, 17, 18

[ ] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 August 2005 (11-08-2005)	22 August 2005 (22-08-2005)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Jeffrey Orser (819) 934-2669

Nintendo Exhibit 1003
Part 1 of 2
Page 00414

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2005/000650

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
WO0177811	18-10-2001	AU5304901 A	23-10-2001
WO03058411 A1	17-07-2003	AU2003201905 A1	24-07-2003
		CN1613040 A	04-05-2005
		EP1465039 A1	06-10-2004
		JP2003202929 A	18-07-2003
		NZ533766 A	24-12-2004
		TW224909 B	01-12-2004
		US2005166264 A1	28-07-2005
		EP1465039	06-10-2004
EP1465041	06-10-2004	CN1534429 A	06-10-2004
		JP2004302963 A	28-10-2004
		US2004260939 A1	23-12-2004
US6513121	28-01-2003	CA2313851 A1	20-01-2001
		EP1071253 A1	24-01-2001
		JP2001067135 A	16-03-2001
US2005050319	03-03-2005	DE102004038566 A1	14-04-2005
		GB0417768D D0	15-09-2004

Nintendo Exhibit 1003
Part 1 of 2
Page 00415

COPY

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
BORDEN LADNER GERVAIS LLP
World Exchange Plaza
1100 - 100 Queen Street
OTTAWA, Ontario
Canada, K1P 1J9

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)* 22 August 2005 (22-08-2005)

Applicant's or agent's file reference
PAT 59029W-90

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/CA2005/000650	29 April 2005 (29-04-2005)	30 April 2004 (30-04-2004)

International Patent Classification (IPC) or both national classification and IPC
IPC(7): G06F 12/14, H04Q 7/32, H04L 9/32, H04M 1/67

Applicant
RESEARCH IN MOTION LIMITED ET AL

1. This opinion contains indications relating to the following items :

[X]	Box No. I	Basis of the opinion
[X]	Box No. II	Priority
[X]	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
[ ]	Box No. IV	Lack of unity of invention
[X]	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
[ ]	Box No. VI	Certain documents cited
[ ]	Box No. VII	Certain defects in the international application
[ ]	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**
If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later. (Nov 22/05)
(Feb 28/06) - entered ge
For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/CA	Date of completion of this opinion	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	16 August 2005 (16-08-2005)	Jeffrey Orser (819) 934-2669

Nintendo Exhibit 1003
Part 1 of 2
Page 00416

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   [X] the international application in the language in which it was filed

   [ ] a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material

      [ ] a sequence listing

      [ ] table(s) related to the sequence listing

   b. format of material

      [ ] on paper

      [ ] in electronic form

   c. time of filing/furnishing

      [ ] contained in the international application as filed.

      [ ] filed together with the international application in electronic form

      [ ] furnished subsequently to this Authority for the purposes of search.

3 [ ] In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statement that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments :

Nintendo Exhibit 1003
Part 1 of 2
Page 00417

Box No. II Priority

1. [ ] The validity of the priority claim has not been considered because the International Searching Authority does not have in its possession a copy of the earlier application whose priority has been claimed or, where required, a translation of that earlier application. This opinion has nevertheless been established on the assumption that the relevant date (Rules 43bis.1 and 64.1) is the claimed priority date.

2. [ ] This opinion has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rules 43*bis*.1 and 64.1). Thus for the purposes of this opinion, the international filing date indicated above is considered to be the relevant date.

3. Additional observations, if necessary :

The priority claim has been considered by the International Searching Authority and found to be valid.

Nintendo Exhibit 1003
Part 1 of 2
Page 00418

Box No. III **Non-establishment of opinion with regard to novelty, inventive step and industrial applicability**

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of :

[ ] the entire international application

[X] claim Nos. 14 and 15

because:

[ ] the said international application, or the said claim Nos. relate to the following subject matter which does not require an international search *(specify)* :

[ ] the description, claims or drawings *(indicate particular elements below)* or said claim Nos. are so unclear that no meaningful opinion could be formed *(specify)* :

[ ] the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed *(specify)*:

[ ] no international search report has been established for said claims Nos.

[ ] a meaningful opinion could not be formed without the sequence listing; the applicant did not, within the prescribed time limit:

[ ] furnish a sequence listing on paper complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.

[ ] furnish a sequence listing in electronic form complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.

[ ] pay the required late furnishing fee for the furnishing of a sequence listing in response to an invitation under Rule 13*ter*.1(a) or (b).

[ ] a meaningful opinion could not be formed without the tables related to the sequence listings; the applicant did not, within the prescribed time limit, furnish such tables in electronic form complying with the technical requirements provided for in Annex C-*bis* of the Administrative Instructions, and such tables were not available to the International Searching Authority in a form and manner acceptable to it.

[ ] the tables related to the nucleotide and/or amino acid sequence listing, if in electronic form only, do not comply with the technical requirements provided for in Annex C-*bis* of the Administrative Instructions.

[X] See Supplemental Box for further details.

Nintendo Exhibit 1003
Part 1 of 2
Page 00419

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	None	YES
	Claims	1-18	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-18	NO
Industrial applicability (IA)	Claims	1-13, 16-18	YES
	Claims	None	NO

2. Citations and explanations :

Reference is made to the following documents:
D1: WO 01/7781 A1 Jooste 18 October 2001 (18-10-2001)
D2: WO 03058411 A1 Yamada et al. 17 July 2003 (17-07-2003)
D3: US 6513121 B1 Serkowski 28 January 2003 (28-01-2003)

For the purpose of the opinion, document D1 is considered as the closest prior art.

Claims 1 and 17
Document D1 discloses application control for use on an electronic device wherein an operation request from an application is received (page 9, lines 7-12), determining whether the requested operation is allowed to be performed by the application based upon a stored authorization record and an application identifier associated with the application (page 14, lines 1-4 and 21-31) and allowing the application to perform the requested operation based upon whether the requested operation is determined to be allowed to be performed by the application (abstract, page 9, lines 9-12).

Claim 2
Document D1 discloses that the application is allowed to perform the requested operation only if the request operation is determined to be allowed to be performed by the application (page 9, lines 13-16).

Claims 3 and 4
Document D1 discloses that the authorization record and the application identifiers are provided by an external source for storage on the electronic device (page 8, lines 17-26 and page 10, line 23 to page 11, line 7) and that they are provided through a wireless communication channel (page 5, lines 2-8 and page 11, lines 1-7).

Claim 5
Document D1 discloses that the authorization record related to determining whether the requested operation is to be allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization (page 10, line 23 to page 11, line 7).

Claim 6
Document D1 discloses an analogous situation to that wherein an update to the authorization record is provided by an external source for storage on the electronic device (page 10, line 23 to page 11, line 7).

Claim 7
Document D1 discloses the situation wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device (page 14, lines 21-29) and determining whether the requested operations are allowed to be performed by their respective applications based and allowing the plurality of applications to perform their respective requested operations (page 14, lines 1-4 and 21-31; abstract; and page 9, lines 9-12).

(continued in Supplemental Box on page 6)

Nintendo Exhibit 1003
Part 1 of 2
Page 00420

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of: Box No. III and Box No. V

Box No. III

The subject matter in claims 14 and 15 pertains to a computer program product and a data signal, respectively, which may be considered excluded matter in certain jurisdictions according to PCT Rule 67.1(vi). As no unified criteria exists under PCT for assessing the industrial applicability of computer program product and data signal claims, thus no opinion with regards to industrial applicability has been provided for claims 14 and 15.

Box No. V

Claim 8
Document D1 discloses an analogous method to grouping two or more applications and associating them with one of the authorization records. More specifically, document D1 categorizes each application as authorized or not authorized (page 18, claim 5). As such an authorization record grouping two or more applications would be within the grasp of a person skilled in the art in view of document D1's disclosure .

Claims 9 and 10
Document D1 discloses that the requested operation are I/O requests for accessing memory (abstract, page 9, lines 3-12 and page 17, lines 20-22).

Claim 11
Document D1 discloses that the stored authorization record is associated with data indicative of whether the application is required, allowed or excluded (page 10, lines 23-28, page 14, lines 1-4 and 21-31).

Claim 12
Document D1 discloses that the authorization record is stored in a protected data store thereby preventing alteration or deletion to the authorization record unless permitted (page 9, lines 3-12).

Claim 13
Document D1 discloses the embodiment wherein the electronic device is a wireless mobile communications device or a personal digital assistant (page 5, lines 2-6).

Claims 14 and 15
Document D1 discloses that "computer-readable medium" and "a carrier wave that encodes a data signal" are recognized embodiments of the disclosed subject-matter (page 7, lines 23-26).

Claim 16
Document D1 discloses that the application operates upon the electronic device (abstract).

Claim 18
Document D1 discloses: receiving an operation request from an application (page 9, lines 7-12) wherein the requested operation is accessing local memory (abstract, page 9, lines 3-12 and page 17, lines 20-22); determining whether the requested operation is allowed to be performed by the application based upon a stored authorization record and an application identifier associated with the application (page 14, lines 1-4 and 21-31) wherein the stored authorization record is associated with data indicative of whether the application is required, allowed or excluded (page 10, lines 23-28, page 14, lines 1-4 and 21-31), wherein the authorization record related to determining whether the requested operation is to be allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization (page 10, line 23 to page 11, line 7); and allowing the application to perform the requested operation based upon whether the requested operation is determined to be allowed to be performed by the application (abstract, page 9, lines 9-12).

(continued in Supplemental Box on page 7)

Nintendo Exhibit 1003
Part 1 of 2
Page 00421

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of: Box No. V

Remarks regarding additionally referenced documents

Document D2 discloses application control for a mobile apparatus which receives an operation request (*installation and activation*, see abstract) from an application (*Java AP-software*, see abstract), determines whether the requested operation is allowed to be performed by the application based upon a stored authorization record and an application identifier associated with the application (*Security Description File*, see abstract and paragraph [0020], and allows the application to perform the requested operation based upon whether the requested operation is determined to be allowed to be performed by the application (see abstract, paragraphs [0006], [0013]).

Document D3 discloses application control on an electronic device (*telecommunication system*, see abstract) wherein an application sends an operation request (see abstract and column 3, lines 9-14) to a licensed server, determination whether the requested operation is allowed to be performed by the application is made based upon a stored authorization record (*license file*, see abstract) and an application identifier associated with the application (see abstract, column 2, lines 13-18) and allowing the application to perform the requested operation based on the comparison of the authorization record and the application identifier (see column 2, lines 15-23).

Conclusions

Novelty and Inventive step

As document D1 discloses all subject-matter recited in claims 1-18, therefore these claims are not deemed to fulfill the requirement of PCT Article 33(2) and PCT Article 33(3).

Industrial applicability

The subject-matter of claims 1-13 and 16-18 is considered to be industrially applicable and thus fulfilling the requirements of PCT Article 33(4).

The subject matter in claims 14 and 15 pertains to a computer program product and a data signal, respectively, which may be considered excluded matter in certain jurisdictions according to PCT Rule 67.1(vi). As no unified criteria exists under PCT for assessing the industrial applicability of computer program product and data signal claims, thus no opinion with regards to industrial applicability has been provided for claims 14 and 15.

Nintendo Exhibit 1003
Part 1 of 2
Page 00422

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 813 132 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
26.01.2005 Bulletin 2005/04

(51) Int Cl.[7]: **G06F 1/00**, G06F 9/46, H04L 29/06

(21) Application number: **97303443.2**

(22) Date of filing: **20.05.1997**

(54) **Support for trusted software distribution**

Unterstützung für die Verteilung von vertrauter Software

Support pour la distribution de logiciels sécurisés

(84) Designated Contracting States:
DE FR GB

(30) Priority: **11.06.1996 US 661517**

(43) Date of publication of application:
17.12.1997 Bulletin 1997/51

(73) Proprietor: **International Business Machines Corporation**
Armonk, N.Y. 10504 (US)

(72) Inventors:
- **Dan, Asit**
  West Harrison, New York 10604 (US)
- **Ramaswami, Rajiv**
  Ossining, New York 10562 (US)
- **Sitaram, Dinkar**
  Yorktown Heights, New York 10598 (US)

(74) Representative: **Waldner, Philip**
IBM United Kingdom Limited,
Intellectual Property Department,
Hursley Park
Winchester, Hampshire SO21 2JN (GB)

(56) References cited:
WO-A-97/07657 **US-A- 5 210 872**
US-A- 5 412 717

- **DEAN D ET AL: "JAVA SECURITY: FROM HOTJAVA TO NETSCAPE AND BEYOND" PROCEEDINGS OF THE 1996 IEEE SYMPOSIUM ON SECURITY AND PRIVACY. OAKLAND, CA., MAY 6 - 8, 1996, PROCEEDINGS OF THE IEEE SYMPOSIUM ON SECURITY AND PRIVACY, LOS ALAMITOS, IEEE COMP. SOC. PRESS, US, vol. SYMP. 17, 6 May 1996 (1996-05-06), pages 190-200, XP000634844 ISBN: 0-7803-3527-9**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 0 813 132 B1

Description

[0001] The present invention relates generally to delivery of software through distribution systems such as networks.

[0002] Software distribution is a major industry currently. Software is today distributed over diskettes, CDROMs and increasingly, over networks. In addition to simply downloading code from remote sites over the Internet, today clients can download and run applets from servers, a paradigm proposed in the Java programming language or in other languages such as Telescript.

[0003] A significant concern with code obtained from elsewhere is that of security. For example, in the Unix operating system, the code will run in the client's shell with all the client's privileges, including access to all his files, as well as possibly send mail, attempt illegal break ins etc. Java attempts to solve this problem for applets by running applets in a very restrictive environment. As a result, the usefulness and functionality of Java applets is limited. Java applications on the other hand rely on the security provided by the operating system and do not come with any degree with authentication. They thus pose the same security problems as any other code.

[0004] A form of authentication is proposed in "Trusted Distribution of Software Over the Internet", A.D. Rubin, Internet Society Symposium on Network and Distributed Security, 1995. Here a trusted third party signs a certificate to identify the author of a program and to secure its integrity. While this allows a client to verify the authenticity of the code, it does not specify a flexible set of permissions associated with the code nor does it provide an automated method for the client to enforce these permissions.

[0005] In a preferred embodiment, a code production system communicates with a certification agency, which is a trusted third party. The certification agency issues a certificate for the code and a certificate for the access list of that code. Once the certificate is issued it is not possible for any party to modify the code or access list without invalidating the certificate. The code and its ACL, along with their certificates are stored on a server. A client downloading the code or access list can verify the integrity of the code/access list and the system can enforce the access list such that the permissions and resources are not exceeded.

[0006] US-A-45412217 discloses a computer system security method and apparatus having program authorization structures.

[0007] US-A-5 412 717 discloses a system monitor which limits the ability of a program about to be executed to the use of predefined resources. A so-called third party certified "program authorization information (PAI)" is associated with the program and contains the restrictions assigned to the program.

[0008] US-A-5 210 872 discloses a task scheduling method which assigns each task a consumption quota and controls each task as it executes by desactivating the a task which consums more than its quota.

[0009] According to one aspect of the present invention there is provided a method for distributing program code comprising the steps of providing to a recipient system a trusted third party certification, the trusted third party certification including a computer readable description of resources and permissions required for verified non-harmful operation of the code,

characterised in that the descriptions of resources required includes data describing both a quantity of each resource to be used by the code and a maximum rate of consumption of each resource by the code.

Figure 1 shows a block-diagram view of a code delivery and certification system according the preferred embodiment of the invention;

Figure 2 shows how the different parts of the client system operate together to perform the functions described in the embodiment;

Figure 3 shows the access control list (ACL);

Figure 4 shows the data structures used by the ACL enforcer;

Figure 5 shows how logical resource permissions are enforced by the ACL enforcer;

Figure 6 shows how physical resource limits are enforced by the ACL enforcer;

Figure 7 shows the pseudocode for the integrity verification, execution and enforcement initialization operations of the client system;

Figure 8 shows the pseudocode for the ACL manager; and

Figure 9 shows the pseudocode for the ACL enforcer.

[0010] Figure 1 shows a block-diagram view of a code delivery and certification system according to a preferred embodiment of the invention. It includes of one or more code production systems (CPS) 10, a certification agency (CA) 15, one or more servers 20 and one or more client systems 30. The client systems can be coupled to the servers by way of a conventional Wide Area Network (WAN) or by way of a Local Area Network (LAN). The CPS has a piece of program code (code) 140 and an access list (ACL) 150 for that code that it wishes to get certified by the certification agency. The CA provides a public key K that is widely available and known to the client system. In addition the CA has a private key P that only it knows. To provide a certificate for the code the CA creates a certificate containing the code name and the cryptographic hash of the code and signs

Nintendo Exhibit 1003
Part 1 of 2
Page 00424

it using his private key. The certificate cannot now be changed without invalidating the CA's signature. Similarly the CA creates and signs another certificate for the ACL associated with that code (if desired there could be a single certificate for both the code and its access list). In the embodiment of Figure 1, the client systems receive the certificate, the ACL and the code by way of the WAN or LAN. It should be understood, however, that the client systems can also or alternatively receive certified code by way of a removable storage media read by local importation device such as a floppy or optical disk drive.

[0011] The client system shown in Figure 2 includes a verifier 110, ACL manager 130, executor 170, ACL enforcer 180 and a client interface 190. The client system also includes a conventional CPU and associated control logic 192, a communication controller/network interface 194, a CD-ROM and/or floppy disk subsystem 196 and other resources such as network access modules, a display subsystem and various special purpose adapters. Those of skill in the art will recognize that the client system includes a number of additional, conventional components which will not be described in detail here.

[0012] The ACL manager 130 and the ACL enforcer 180 are preferably embodied as program code, the operation of which is described in more detail below. The executer is a conventional part of the client's operating system (not shown) which is used to execute the imported code on the client system. The client interface 190 can be embodied as a front of screen graphical user interface which provides the client communication with the ACL manager (e.g. it enables the client to tell the ACL manager 130 to allow or disallow or control program access to specified resource). The verifier 110 is preferably embodied as program code including a decryption module which is used to verify the authenticity of the imported code, including the access control list. The verifier also includes a hashing module which checks the integrity of the imported code and ACL.

[0013] Upon downloading the code/ACL and its certificate (100), the verifier (110) first checks to see if the CA's signature on the certificate is valid (using CA's known public key). The verifier then computes the cryptographic hash of the code/ACL and verifies that it matches the value in the certificate. If the signature is not valid or the hash does not match, the code and ACL are rejected (120). If the verification is ok, the ACL manager (130) is invoked. The ACL manager displays the ACL (described below) to the client via the client interface (190) and ascertains whether the client wishes to allow or disallow the individual items in the ACL. The ACL manager stores the code (140) as directed by the client via the client interface and stores the ACL (150) together with permission flags (160).

[0014] The resources that can have their access controlled by the ACL enforcer include both logical resources such as filesystems, specific files and system calls, as well as physical resources including such things as the disk space, disk access, main memory allocation and access to various system controllers and adapters. For access to logical resources (client system facilities), the permission flags 160 indicate whether individual items are allowed or not; for access to physical resources, the permission flags can be used to indicate the maximum allowable quantity or rate of consumption.

[0015] Figure 2 also shows how the different parts of the client system operate together. In a multi-user client system, each user may have their own set of permission flags. The ACL may also contain environment variables; changing the environment variables during execution allows individual users to customize the access privileges. The ACL and permission flags are stored in a secure area; reading or updating this area is a privilege enforced by the ACL enforcer (180).

[0016] The ACL manager may be invoked at any time by the client to display or change the permissions of an ACL. The code is run by the executor (170). Before allowing access to any resource, the executor invokes the ACL enforcer for checking the validity of the access. This is achieved by the executor 170 inserting traps in the code to a verification routine that invokes the ACL enforcer. The operation of the ACL enforcer is described in more detail later.

[0017] The system enables the code and its ACL to be downloaded separately or together as needed. For instance, the CPS may want to provide the ACL free of charge to all clients but charge for the actual code.

[0018] Figure 3 shows the access control list. The ACL consists of two parts: the Physical Resources Table (PRT) 200 containing the physical resources required by the code and the Logical Resources Table (LRT) 250 containing the permissions and logical resources required by the code.

[0019] The PRT 250 contains a row for each resource containing the physical resource name (PRN) 205, the resource attribute 210, the maximum consumption rate 215 and the maximum amount 220. The resource attribute 210 is used when a physical device or resource disk has multiple attributes, such as space and number of I/Os for storage devices. The maximum consumption rate 215 and the maximum amount 220 are the maximum allowable consumption rate and maximum allowable consumption of the resource and attribute respectively.

[0020] The LRT 250 contains a row for each call to an external routine required by the code (referred to as a logical resource). Each row contains the logical resource name (LRN) 255, and a parameter list 260 that points to a list of parameter entries. Each parameter entry 265 specifies a set of valid parameter ranges; i.e. a set of values for each parameter that are valid in combination, together with a field nextPE 280 that points to the next parameter entry. The parameter range for each parameter contains two fields - the parameter type 270 and the parameter value 275 that specifies the valid range for that parameter. For string parameters, the parameter type 270 is STR and the parameter value 275

Nintendo Exhibit 1003
Part 1 of 2
Page 00425

is a list of regular expression that specify valid forms for the string. For integer parameters, the parameter type 270 is INT and the parm. value 275 is a list of integer ranges. The parm. value 275 may include the names of environment variables, in which case the environment variable is assumed to contain a value which is substituted at run time.

[0021] The ACL enforcer in the client ensures that the permissions and resources specified in the ACL for the code are provided and no additional permissions/resources are allowed.

[0022] The ACL enforcement may be static or dynamic. In static enforcement, the enforcement can be done fully before the code is executed and no enforcement is required while the code is running. In dynamic enforcement, the enforcement must be performed while the code is being executed. If the CA itself verifies the ACL and guarantees that they will not be exceeded by the code, then the ACL enforcement function may not be required in the client system.

[0023] Figure 4 shows the data structures used by the ACL enforcer. The Runtime Physical Resources Table (RPRT) 300 contains a row for each resource. The resource name 300, resource attribute 310, maximum consumption rate 315 and maximum amount 320 are copies of the corresponding fields from the PRT 200. The actual consumption rate 325 and the actual use 330 fields are used to keep track of the actual consumption rate and the actual consumption, respectively, of the code during run time. The Runtime Logical Resource Table (RLRT) 350 contains a row for each required logical resource. The RLRT is a copy of the LRT, with an additional flag that indicates for each valid combination of parameters, whether the combination is allowed by the ACL manager or not. The Logical Resource Name 355 is a copy of the corresponding fields of the LRT 250 and the parameter list 360 points to a list of runtime parameter entries (RPE) 365. The parameter type 370, parameter value 375 values of the runtime parameter entries are copies of the corresponding fields in the LRT. The nextPE 380 points to the next runtime parameter entry 365 and the allow 385 field may be set to YES or NO indicating whether this runtime parameter entry 365 is allowed or not.The ACL enforcer also keeps track of the code start time 395.

[0024] Figure 5 shows how logical resource permissions are enforced by the ACL enforcer. This path is invoked whenever the code makes a call to an external function. In step 410, the ACL enforcer locates the number of parameters, their values, and the name of the function being invoked. The exact method for doing this is implementation dependent; for example, in Java, these are located on the operand stack. In step 415, the ACL enforcer locates the row for this function in the RLRT 350 and locates the first RPE 365 with allow set to YES. If the function name is not found, or there is no such RPE 365, the ACL enforcer proceeds to step 455 where it exits indicating that the call is not allowed. In step 420, the ACL enforcer locates the value of the first parameter and makes that the current parameter. In step 425, the ACL enforcer checks if the value of the current parameter is allowed by the RPE 365. If the value is allowed, the ACL enforcer checks in step 430 if there are more parameters. If there are, in step 435 the ACL enforcer sets the current parameter to the next parameter and returns to step 425. If no more parameters are found in step 430, the ACL enforcer proceeds to step 450 and returns with an indication that the call is allowed.

[0025] If the test for allowability fails in step 425, the ACL enforcer proceeds to step 445 where it checks the RLRT 350 to find another RPE 365 with allow 385 set to YES. If there is no such RPE, the ACL enforcer proceeds to step 455 and exits indicating that the call is not allowed. If there is such an RPE 365, the ACL enforcer proceeds to step 420.

[0026] Figure 6 shows how physical requirements are enforced by the ACL enforcer. The ACL enforcer is invoked in step 500 before allocating the resource. Two parameters, the amount of the resource requested (REQAMT) and the estimated time of consumption (COMPT) are provided. For disk I/O, the REQAMT is the amount of disk I/O and the COMPT is the estimated time for the I/O to complete. In step 505, the ACL enforcer locates the row in the RPRT 300 for this resource and checks whether the maximum amount 320 is specified and the actual use 330 plus REQAMT exceeds the maximum amount 320. If so, it returns a failure in step 527 indicating that the consumption is not allowed. If the maximum amount 320 is not exceeded, in step 510 the ACL enforcer computes the projected consumption rate of this resource as (Actual use 330 + REQAMT)/(current time - code start time 395 + COMPT) . In step 515, the ACL enforcer checks to see if the maximum consumption rate 315 is specified and if the projected consumption rate is greater than the maximum consumption rate 315. If the maximum consumption rate 315 is not specified or the projected consumption rate is not greater, the ACL enforcer returns with an indication that the consumption is allowed. If the projected consumption rate is greater, the ACL enforcer in step 530 computes the required delay for performing this operation as (actual use 300 + REQAMT)/maximum consumption rate 315 -(current time - code start time 395 -COMPT) and returns the required delay with an indication that the consumption has to be delayed for the computed delay.

[0027] In step 550, the ACL enforcer is invoked after the consumption of the resource with a parameter specifying the amount of resource consumed (CONSAMT). The ACL enforcer then updates the actual consumption rate 325 and the actual use 330.

[0028] It is also possible for different users to be allocated different resources and permissions in the recipient system for the same code. This can be done either at the time the code is installed, by the ACL manager by looking at the privileges given to the different users and

combining that with the resources and permissions allowed to the code. In this case the set of resources and permissions for each user would have to be stored separately. During code execution the resources and permissions would be enforced on a per-user basis. Alternatively the resources and permissions can be determined during execution of the code by the ACL enforcer by looking at the privileges given to the different users and combining that with the resources and permissions allowed to the code.

[0029] Figure 7 shows the pseudocode for the integrity verification, execution and enforcement initialization operations of the client system. It should be understood that the various tables, lists flags and other data structures described herein are instantiated in the memory of the client system (e.g. in volatile random access memory, disk or a combination of both). As previously discussed, the ACL enforcer and ACL manager are preferably embodied as program code which is linked or incorporated into the operating system of the client system. Figure 8 shows pseudocode for the ACL manager. Figure 9 shows pseudocode for the ACL enforcer.

[0030] Now that the invention has been described by way of the preferred embodiment, various modifications and improvements will occur to those of skill in the art. Thus, it should be understood that the preferred embodiment has been provided as an example and not as a limitation of the claims.

[0031] In summary, there is described a form of authentication is provided wherein a trusted third party signs a certificate to identify the author of a program and to secure its integrity. The program code is encapsulated or otherwise associated with the certificate and an access control list (ACL). The access control list describes the permissions and resources required by the code. An enforcement mechanism which allocates system permissions and resources in accordance with the ACL. In a preferred embodiment, a code production system communicates with a certification agency, which is a trusted third party. The certification agency issues a certificate for the code and a certificate for the access list of that code. Once the certificate is issued it is not possible for any party to modify the code or access list without invalidating the certificate. The code and its ACL, along with their certificates are stored on a server. A client downloading the code or access list can verify the integrity of the code/access list and the system can enforce the access list such that the permissions and resources are not exceeded.

Claims

1. A method for distributing program code comprising the steps of providing to a recipient system (30) a trusted third party certification (150), the trusted third party certification (150) including a computer readable description of resources and permissions required for verified non-harmful operation of the code (200),

   characterised in that the descriptions of resources required includes data describing both a quantity of each resource to be used by the code and a maximum rate of consumption of each resource by the code.

2. The method of Claim 1 wherein the proving comprising the step of encapsulating the certification with the program code.

3. The method of Claim 1 or 2 comprising the further steps of reading (410) the certification by the recipient system; and, allocating (520) resources and permissions of the recipient system so as not to exceed the permissions specified in the certification.

4. The method of Claim 1, 2 or 3 comprising the further steps of denying or granting the code access and permissions to resources of the recipient system in further accordance with user selected options associated with the certification.

5. The method of any of Claims 1 to 4 wherein the computer readable description of resources and permissions is provided to the recipient system in an encrypted form.

6. The method of any of Claims 1 to 5 wherein the certification further includes encrypted verification data and wherein the recipient system decrypts the verification data to verify the integrity of the description of the resources and permissions.

7. The method of any of Claims 1 to 6, wherein the descriptions of permissions required includes data describing specific facilities of the recipient system to be accessed by the code.

8. The method of any of Claims 1 to 7 wherein the third party certification includes a description of the functionality of the code as verified by the third party.

9. The method of any of Claims 1 to 8 wherein the program code is an applet downloaded from a server as a program object.

10. The method of claims 1 to 8 wherein different users are allocated different resources and permissions in the recipient system for the same code.

11. The method of Claim 10 wherein the set of resources and permissions allowed to different users is determined during installation of the code or during execution of the code.

Nintendo Exhibit 1003
Part 1 of 2
Page 00427

Patentansprüche

1. Verfahren für die Verteilung von Programmcode, das die Schritte umfasst, mit denen einem Empfängersystem (30) eine vertrauenswürdige Fremd-Zertifizierung (150) zur Verfügung gestellt wird, wobei die vertrauenswürdige Fremd-Zertifizierung (150) eine computerlesbare Beschreibung der Betriebsmittel und Berechtigungen beinhaltet, die für die nachgewiesenermaßen ungefährliche Ausführung des Codes (200) notwendig sind,
dadurch gekennzeichnet, dass die Beschreibungen der erforderlichen Betriebsmittel Daten beinhalten, die sowohl eine Mengenangabe zu einem jeden Betriebsmittel beschreiben, das von dem Code genutzt wird, als auch eine maximale Verbrauchsrate eines jeden Betriebsmittels durch den Code.

2. Verfahren nach Anspruch 1, wobei die Bereitstellung den Schritt der Kapselung der Zertifizierung mit dem Programmcode umfasst.

3. Verfahren nach Anspruch 1 oder 2, das die weiteren Schritte des Lesens (410) der Zertifizierung durch das Empfängersystem und des Zuweisens (520) von Betriebsmitteln und Berechtigungen des Empfängersystems auf eine Art und Weise umfasst, dass die in der Zertifizierung vorgegebenen Berechtigungen nicht überschritten werden.

4. Verfahren nach Anspruch 1, 2 oder 3, das die weiteren Schritte umfasst, mit denen dem Code Zugriff auf und Berechtigungen für die Betriebsmittel des Empfängersystems verweigert oder gestattet wird bzw. werden, wobei vom Benutzer ausgewählte, der Zertifizierung zugehörige Optionen berücksichtigt werden.

5. Verfahren nach einem beliebigen der Ansprüche 1 bis 4, wobei die computerlesbare Beschreibung der Betriebsmittel und Berechtigungen dem Empfängersystem in verschlüsselter Form bereitgestellt wird.

6. Verfahren nach einem beliebigen der Ansprüche 1 bis 5, wobei die Zertifizierung weiterhin verschlüsselte Prüfdaten beinhaltet und wobei das Empfängersystem die Prüfdaten entschlüsselt, um so die Unversehrtheit der Beschreibung der Betriebsmittel und Berechtigungen zu überprüfen.

7. Verfahren nach einem beliebigen der Ansprüche 1 bis 6, wobei die Beschreibungen der erforderlichen Berechtigungen Daten beinhalten, die bestimmte Leistungsmerkmale des Empfängersystems beschreiben, auf die durch den Code zugegriffen werden soll.

8. Verfahren nach einem beliebigen der Ansprüche 1 bis 7, wobei die Fremd-Zertifizierung eine Beschreibung der Funktionalität des Codes beinhaltet, wie diese durch die Fremdpartei geprüft wurde.

9. Verfahren nach einem beliebigen der Ansprüche 1 bis 8, wobei der Programmcode ein Applet ist, das als ein Programmobjekt von einem Server heruntergeladen wurde.

10. Verfahren nach einem beliebigen der Ansprüche 1 bis 8, wobei verschiedenen Benutzern für denselben Code unterschiedliche Betriebsmittel und Berechtigungen des Empfängersystems zugewiesen werden.

11. Verfahren nach Anspruch 10, wobei der unterschiedlichen Benutzern zur Verfügung gestellte Satz an Betriebsmitteln und Berechtigungen während der Installation des Codes oder während der Ausführung des Codes festgelegt wird.

Revendications

1. Procédé destiné à distribuer un code de programme comprenant les étapes consistant à fournir à un système destinataire (30) une certification d'une tierce partie de confiance (150), la certification de tierce partie de confiance (150) comprenant une description compréhensible par un ordinateur des ressources et des autorisations requises pour une mise en oeuvre avérée non nuisible du code (200), **caractérisé en ce que** les descriptions des ressources requises comprennent des données décrivant à la fois une quantité de chaque ressource à utiliser par le code et un taux maximum de consommation de chaque ressource par le code.

2. Procédé selon la revendication 1, dans lequel la fourniture comprend l'étape consistant à encapsuler la certification avec le code de programme.

3. Procédé selon la revendication 1 ou 2, comprenant les étapes supplémentaires consistant à lire (410) la certification par le système destinataire, et à allouer (520) des ressources et des autorisations du système destinataire de façon à ne pas dépasser les autorisations spécifiées dans la certification.

4. Procédé selon la revendication 1, 2 ou 3 comprenant les étapes supplémentaires consistant à refuser ou à accorder l'accès au code et les autorisations pour les ressources du système destinataire en outre en accord avec des options sélectionnées par l'utilisateur associées à la certification.

5. Procédé selon l'une quelconque des revendications

Nintendo Exhibit 1003
Part 1 of 2
Page 00428

1 à 4, dans lequel la description compréhensible par un ordinateur des ressources et des autorisations est procurée au système destinataire sous une forme cryptée.

6. Procédé selon l'une quelconque des revendications 1 à 5, dans lequel la certification comprend en outre des données de vérification cryptées et dans lequel le système destinataire décrypte les données de vérification pour vérifier l'intégrité de la description des ressources et des autorisations.

7. Procédé selon l'une quelconque des revendications 1 à 6, dans lequel les descriptions des autorisations requises comprennent des données décrivant des modules spécifiques du système destinataire auquel le code doit accéder.

8. Procédé selon l'une quelconque des revendications 1 à 7, dans lequel la certification de tierce partie comprend une description de la fonctionnalité du code telle que vérifiée par la tierce partie.

9. Procédé selon l'une quelconque des revendications 1 à 8, dans lequel le code de programme est une petite application (applet) téléchargée depuis un serveur sous forme d'un objet programme.

10. Procédé selon les revendications 1 à 8, dans lequel différents utilisateurs se voient allouer des ressources et des autorisations différentes dans le système destinataire pour le même code.

11. Procédé selon la revendication 10, dans lequel l'ensemble des ressources et des autorisations allouées à des utilisateurs différents est déterminé pendant l'installation du code ou pendant l'exécution du code.

Nintendo Exhibit 1003
Part 1 of 2
Page 00429

FIG. 1

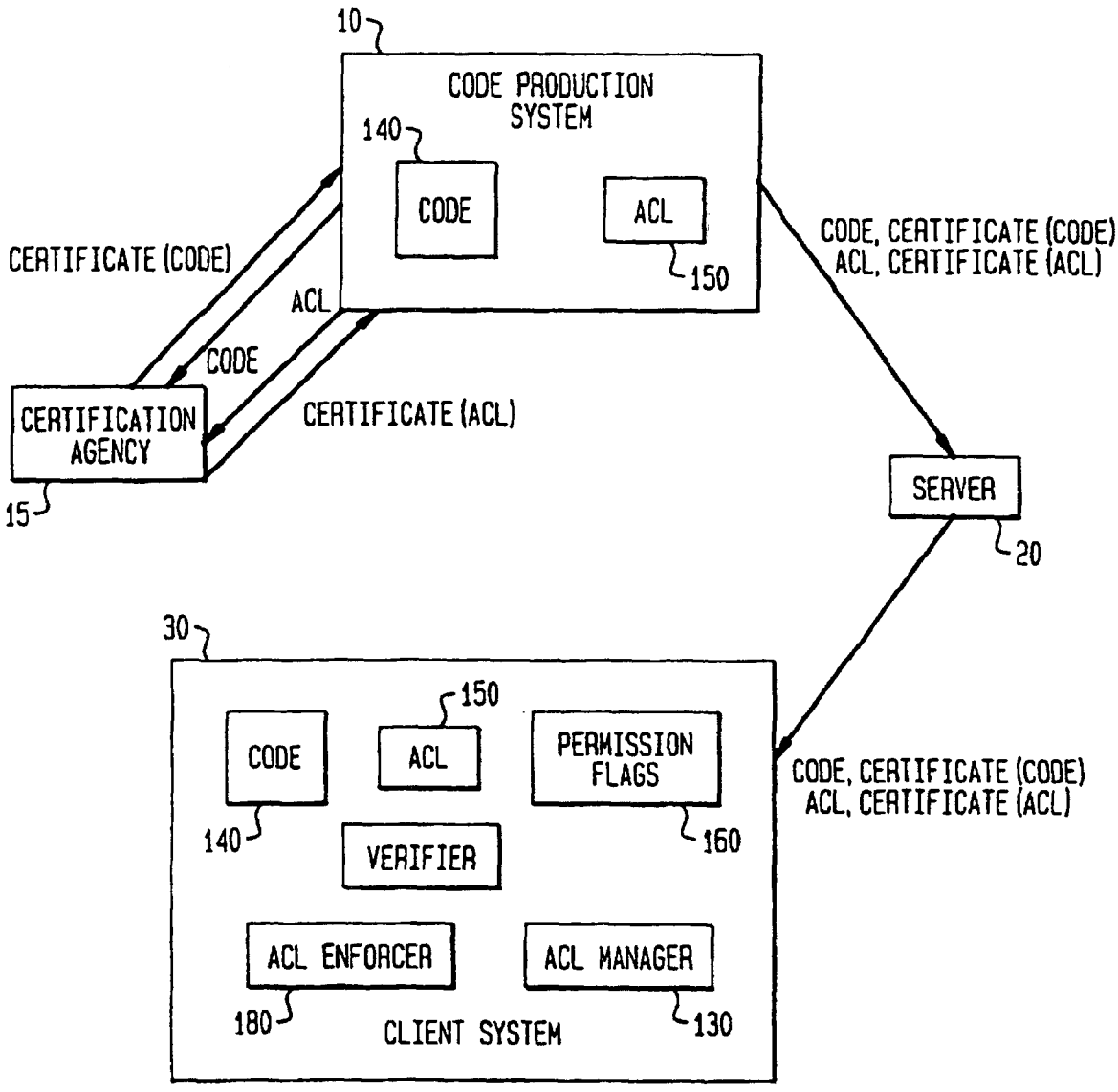
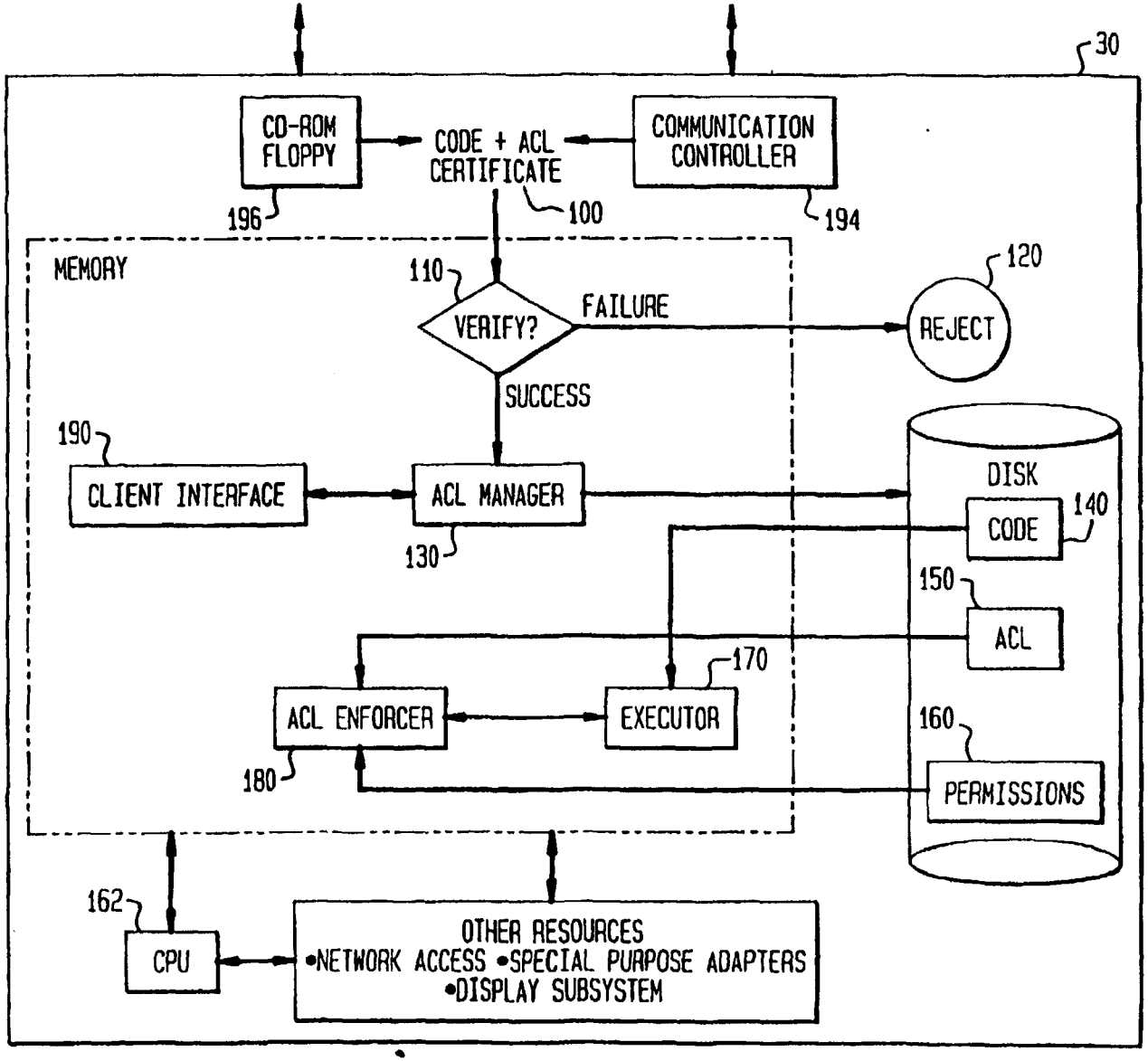

10
CODE PRODUCTION SYSTEM
140
CODE
ACL
150
CERTIFICATE (CODE)
ACL
CODE
CERTIFICATION AGENCY
15
CERTIFICATE (ACL)
CODE, CERTIFICATE (CODE)
ACL, CERTIFICATE (ACL)
SERVER
20
30
150
CODE
ACL
PERMISSION FLAGS
140
160
VERIFIER
ACL ENFORCER
ACL MANAGER
180
130
CLIENT SYSTEM
CODE, CERTIFICATE (CODE)
ACL, CERTIFICATE (ACL)

FIG. 2



EP 0 813 132 B1

FIG. 3

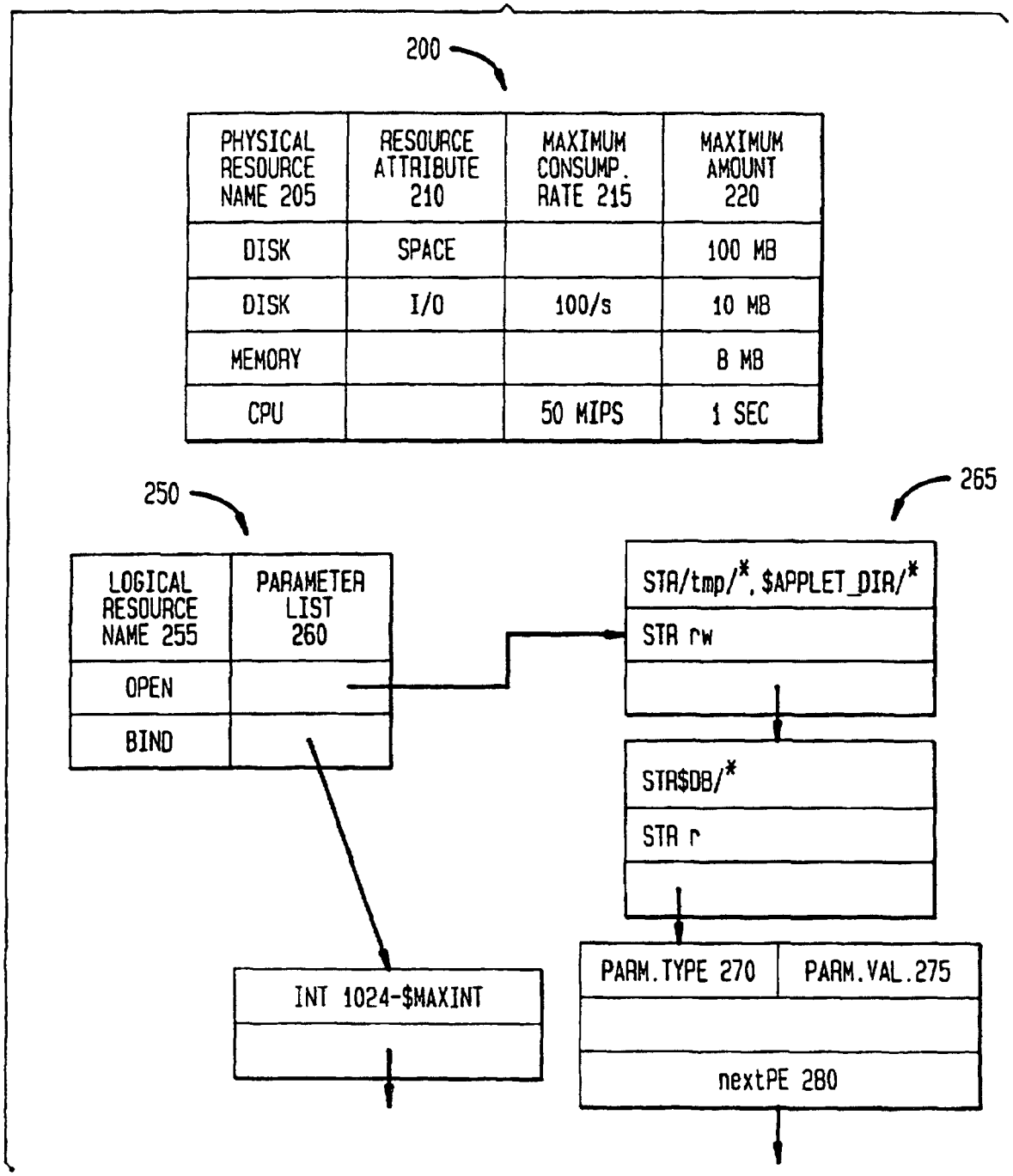

200
PHYSICAL RESOURCE NAME 205
RESOURCE ATTRIBUTE 210
MAXIMUM CONSUMP. RATE 215
MAXIMUM AMOUNT 220
DISK
SPACE
100 MB
DISK
I/O
100/s
10 MB
MEMORY
8 MB
CPU
50 MIPS
1 SEC
250
LOGICAL RESOURCE NAME 255
PARAMETER LIST 260
OPEN
BIND
265
STR/tmp/*, $APPLET_DIR/*
STR rw
STR$DB/*
STR r
INT 1024-$MAXINT
PARM.TYPE 270
PARM.VAL.275
nextPE 280

FIG. 4

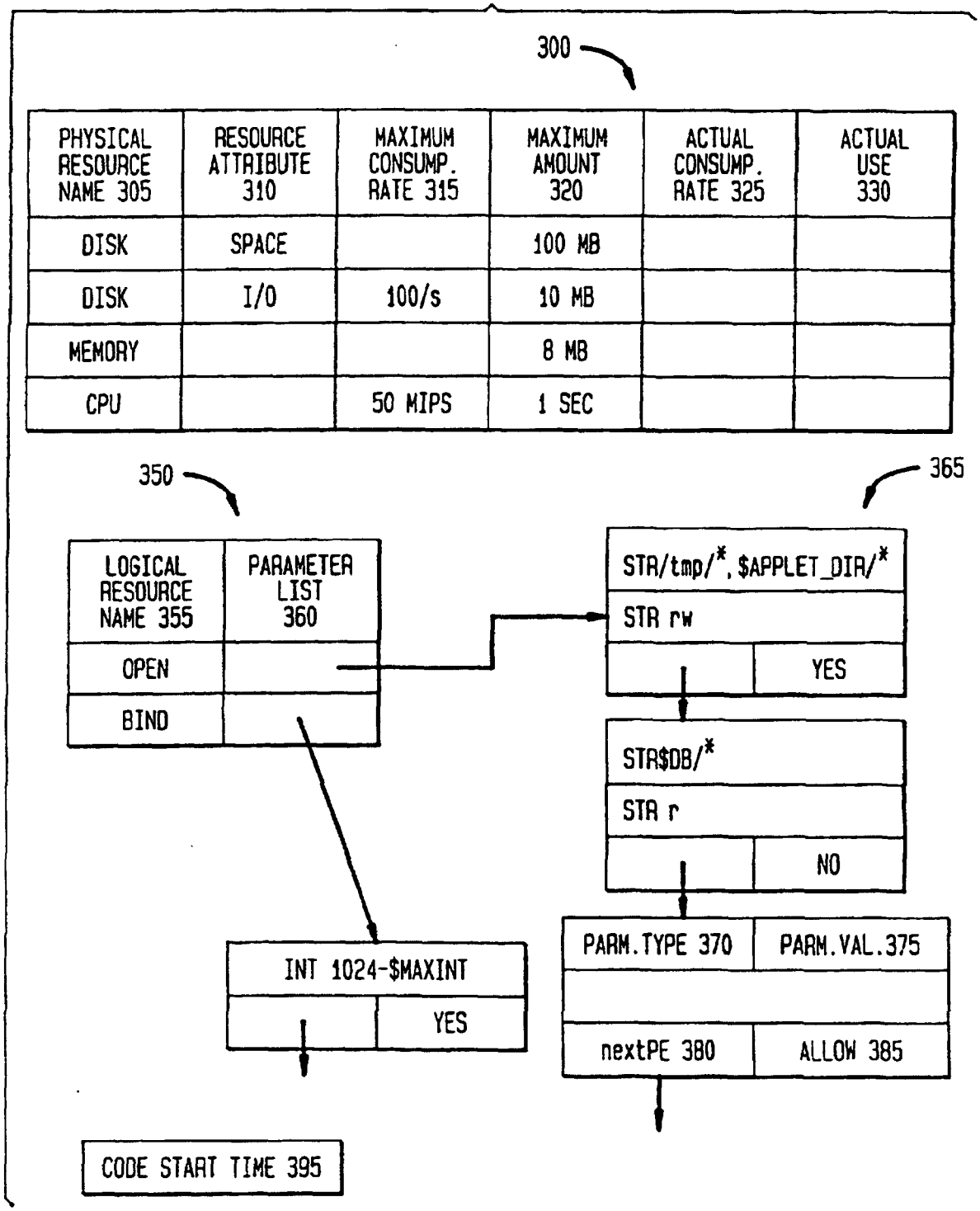

300
PHYSICAL RESOURCE NAME 305
RESOURCE ATTRIBUTE 310
MAXIMUM CONSUMP. RATE 315
MAXIMUM AMOUNT 320
ACTUAL CONSUMP. RATE 325
ACTUAL USE 330
DISK
SPACE
100 MB
DISK
I/O
100/s
10 MB
MEMORY
8 MB
CPU
50 MIPS
1 SEC
350
365
LOGICAL RESOURCE NAME 355
PARAMETER LIST 360
OPEN
BIND
STR/tmp/*, $APPLET_DIR/*
STR rw
YES
STR$DB/*
STR r
NO
INT 1024-$MAXINT
YES
PARM.TYPE 370
PARM.VAL.375
nextPE 380
ALLOW 385
CODE START TIME 395

FIG. 5

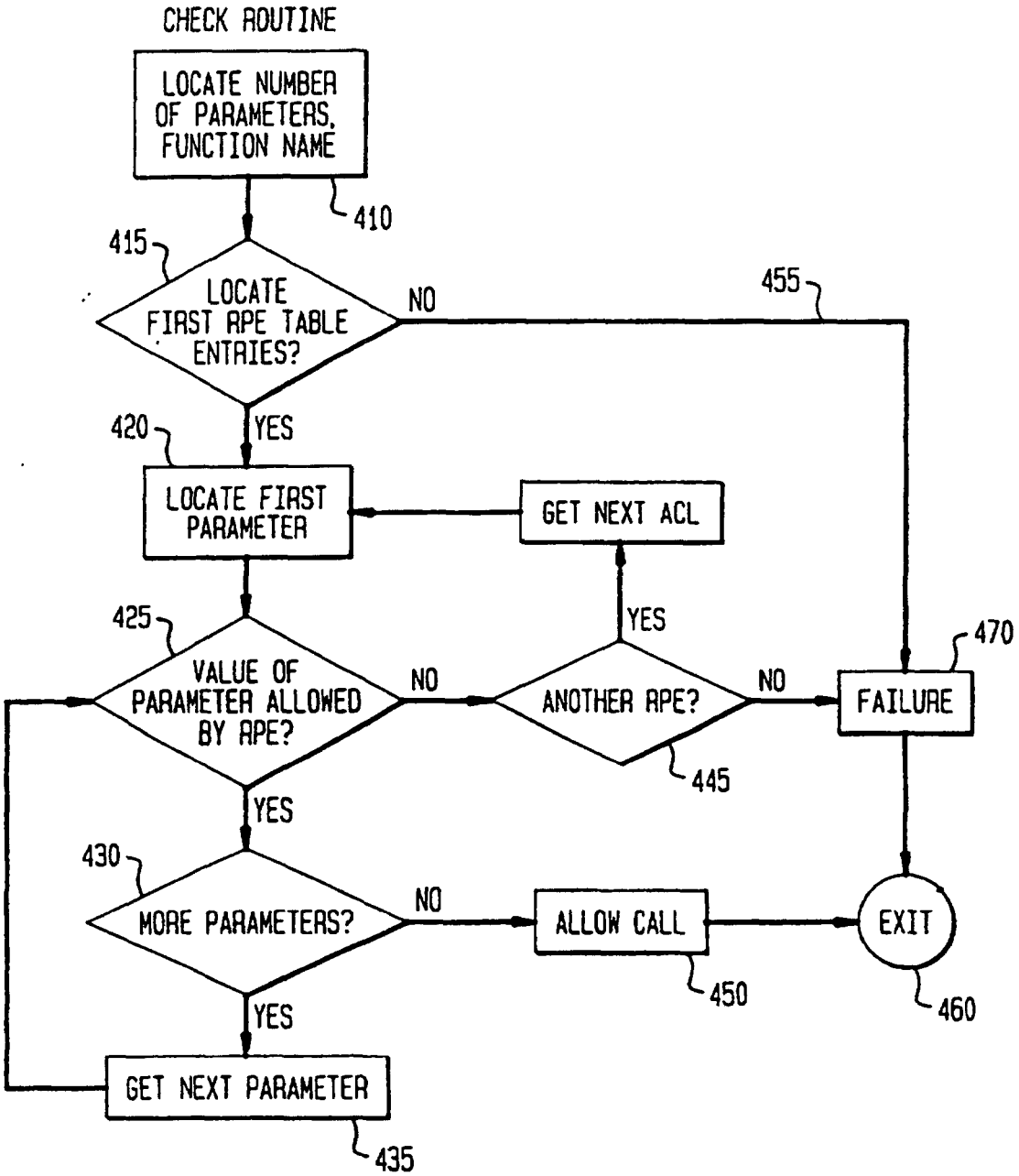

CHECK ROUTINE
LOCATE NUMBER OF PARAMETERS, FUNCTION NAME
410
415
LOCATE FIRST RPE TABLE ENTRIES?
NO
455
YES
420
LOCATE FIRST PARAMETER
GET NEXT ACL
425
VALUE OF PARAMETER ALLOWED BY RPE?
NO
YES
ANOTHER RPE?
NO
445
470
FAILURE
YES
430
MORE PARAMETERS?
NO
ALLOW CALL
450
EXIT
460
YES
GET NEXT PARAMETER
435

FIG. 6

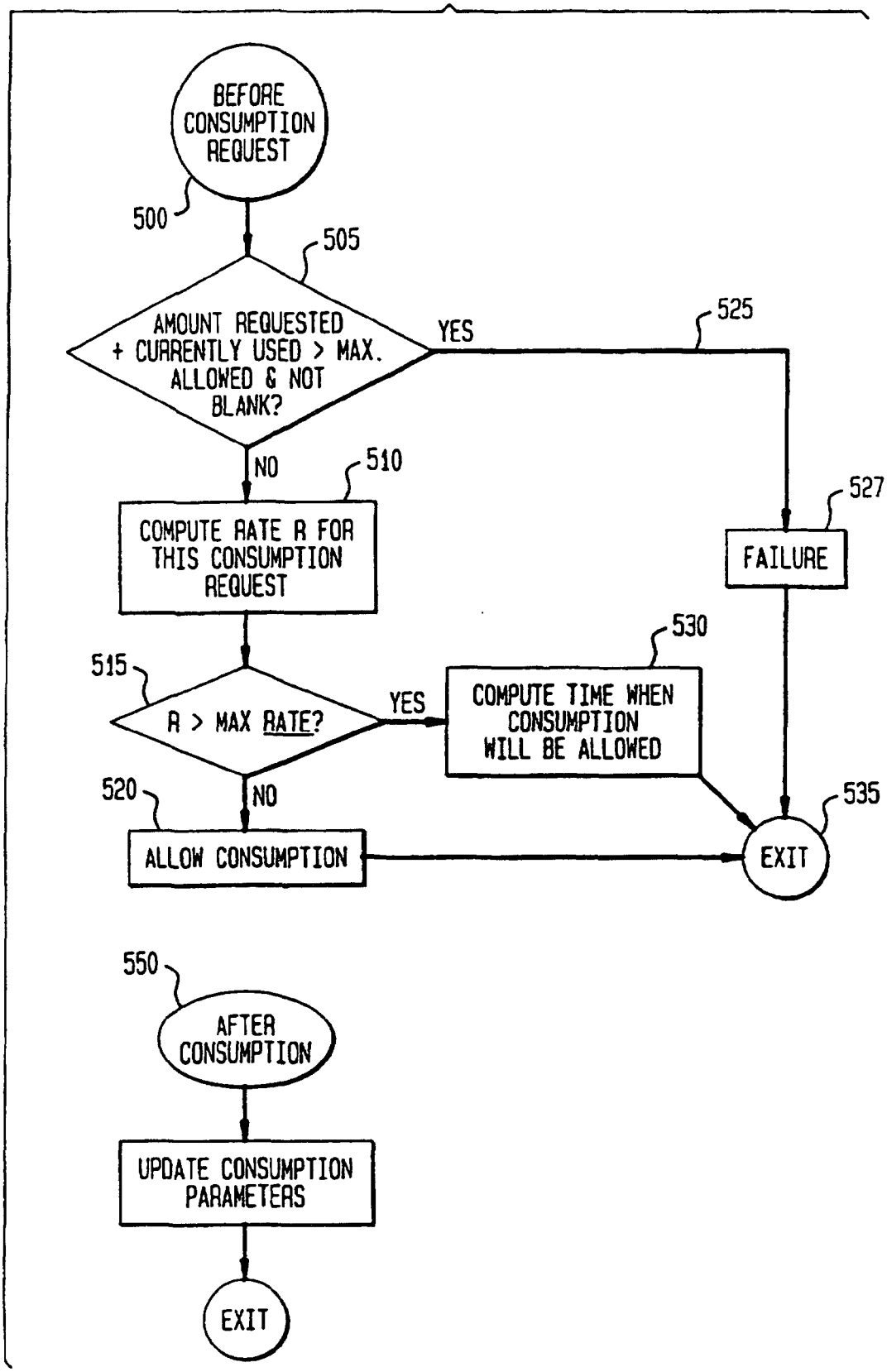

BEFORE CONSUMPTION REQUEST
500
505
AMOUNT REQUESTED + CURRENTLY USED > MAX. ALLOWED & NOT BLANK?
YES
525
NO
510
COMPUTE RATE R FOR THIS CONSUMPTION REQUEST
527
FAILURE
530
515
R > MAX RATE?
YES
COMPUTE TIME WHEN CONSUMPTION WILL BE ALLOWED
NO
520
535
ALLOW CONSUMPTION
EXIT
550
AFTER CONSUMPTION
UPDATE CONSUMPTION PARAMETERS
EXIT

FIG. 7

```
install_code:
-------------

   Receive program code, ACL and encrypted hash;
   Decrypt using third party's public key.
   Compute hash from code and ACL;
   if computed_hash not equal decrypted_hash then
      Reject code;
      exit;
   invoke ACL manager;

execute_code:
-------------

   Insert traps in code to verify_access whenever
resource is accessed;   Execute modified code;

verify_access:
-------------

   Invoke ACL enforcer;
   If access permitted then
      continue;
   else if access delayed then
      delay program;
   else if access rejected then
      suspend program;
```

FIG. 8

```
If newly received code then
   Store code and ACL on disk;
Display ACL for program;
while more client input do
   read client input;
   Modify appropriate permission flags;
   Store modified permission flags on disk;
end
```

FIG. 9

```
check_logical_res_access:
-------------------------

   Locate RPE entries for this logical resource;
   while more RPE entries do
     while more parameters do
        if access to parameter not allowed then
           goto getNextRPE;
     end
     return access allowed;

     getNextRPE: get next RPE;
   end
   return access rejected;

check_physical_res_access:
--------------------------

   Locate RPRT entry for this physical resource;
   if Max_allowed non-blank and amt.requested + used >
max allowed then       return access rejected;
   Computed projected consumption rate;
   if projected consumption rate > max. consumption
rate then       Compute required delay;
     return access delayed and required delay;
  else
     return access allowed;
```

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 828 209 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
11.03.1998 Bulletin 1998/11

(51) Int. Cl.[6]: **G06F 1/00**

(21) Application number: **97115349.9**

(22) Date of filing: **04.09.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **04.09.1996 KR 9638280**

(71) Applicant:
Samsung Electronics Co., Ltd.
Suwon City, Kyungki-do (KR)

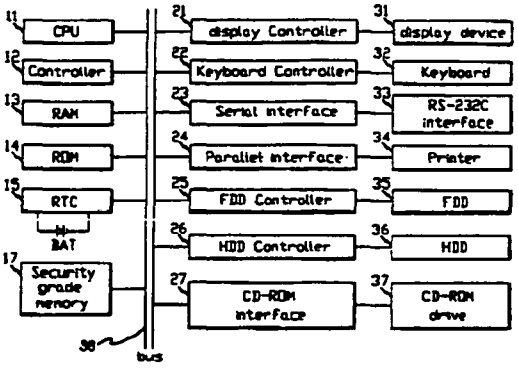
(72) Inventor: **Lee, Sang-Jin**
Kwonsen-gu, Suwon-city, Kyungki-do (KR)

(74) Representative:
Herrmann-Trentepohl, Werner, Dipl.-Ing.
Patentanwälte
Herrmann-Trentepohl
Grosse - Bockhorni & Partner
Forstenrieder Allee 59
81476 München (DE)

(54) A computer system having a function for intercepting lewd/violent programs and method for controlling access of such lewd/violent programs

(57) A computer system having a function of interrupting lewd/violent programs which includes a read-only-memory for storing an initialization program and a security grade setup program; a non-volatile memory device for storing a security grade which is a program classification code selected by a user for designating an unacceptable program content contained in an application program, and a password for identifying the user when changing the security grade; and a controller for controlling execution of an application program according to the security grade of the application program and the security grade stored in the non-volatile memory device during initialization, and for controlling the changing of the security grade stored in the non-volatile memory device during the security grade setup, when the user inputs a password that corresponds to the password stored in the non-volatile memory device. As a result, the computer system is able to limit access to application programs that contain unacceptable levels of graphic sex, violence, and strong language.

FIG.2



EP 0 828 209 A2

Printed by Xerox (UK) Business Services
2.15.12/3.4

BNSDOCID <EP ___ 0828209A2 I >

Nintendo Exhibit 1003
Part 1 of 2
Page 00438

Description

CLAIM FOR PRIORITY

This application makes reference to, incorporates the same herein, and claims all benefits accruing under 35 U.S.C. §119 from an application for *A COMPUTER HAVING A FUNCTION FOR INTERCEPTING LEWD/VIOLENT PROGRAMS AND THE CONTROLLING METHOD THEREOF* earlier filed in the Korean Industrial Property Office on the 4th of September 1996, and there duly assigned Serial No. 38280/1996, a copy of which application is annexed hereto.

BACKGROUND OF THE INVENTION

Technical Field

The present invention relates to a computer system having a function for intercepting lewd/violent programs, and more particularly, relates to a computer system capable of executing application programs according to a set security grade and an application program grade and a method for controlling access of such application programs.

Related Art

Computer programs available for home multi-media computer systems today, like their predecessor video programs for viewing on television receivers, video cassette recorders, and cable boxes, vary greatly in their content of such things as violence, nudity, depictions of sexual acts, strong language, or other things many people may regard as obscene or otherwise objectionable. Many pornographic or extremely violent computer game programs intended for adults have become readily accessible to unintended audiences such as teenagers and children, and increasingly unmanageable by distributors and parents.

Unlike television receivers, video cassette recorders, and cable boxes in which parental control systems and censorship supervision systems are available for parents to control the video viewing of undesirable programs however, home computer systems have not provided parents with a comprehensive control over pornographic or extremely violent computer programs which may be accessed by teenagers and children left unattended at home. For example, contemporary parental control techniques for television receivers and cable boxes are disclosed in U.S. Patent No. 4,930,160 for *Automatic Censorship Of Video Programs* issued to Vogel, U.S. Patent No. 5,382,983 for *Apparatus And Method For Total Parental Control Of Television Use* issued to Kwoh et al., U.S. Patent No. 5,387,942 for *System For Controlling Reception Of Video Signals* issued to Lemelson, U.S. Patent No. 5,485,518 for *Electronic Media Program Recognition And Choice* issued to Hunter et al., U.S. Patent No. 5,550,575 for *Viewer Discretion Television Program Control System* issued to West et al., U.S. Patent No. 5,583,576 for *Rating-Dependent Parental Lock-Out For Television Reception* issued to Perlman et al. Video viewing censoring systems for video cassette recorders may be disclosed, for example, in U.S. Patent No. 5,214,556 for *Video Cassette Recorder Protection System* issued to Kilbel, and U.S. Patent No. 5,548,345 for *Video Viewing Censoring Supervision System* issued to Brian et al. In general, there are essentially two techniques to parental control of viewing of undesirable video programs on televisions or video cassette recorders. The first technique requires participation of individuals at home to invariably control admission of video programs that fail to satisfy their own content criteria. The second technique requires participation of broadcasters in what is generally termed a "V-chip" approach. A program classification code which represents an arbitrary number of designations for rating the program content according to levels of violence, graphic sex, obscenity or other undesirable content is encoded into a video signal for transmission purposes. Before reaching the picture generation elements of the television receiver, the video signal is received by control circuitry which extracts the program classification code therefrom for comparison with a preselected reception code which represents the program content which is desired to either block or allow the reception of the video signal by the television receiver.

Despite of a litany of parental control and censorship supervision systems that are available for television receivers, video cassette recorders and cable boxes, I have observed however, that none is provided for home computer systems. Consequently, there is no effective means currently available for home computer systems to limit access to pornographic programs or extremely violent computer games.

SUMMARY OF THE INVENTION

Accordingly, it is therefore an object of the present invention to provide a computer system capable of limiting access to undesirable computer programs such as pornographic programs or extremely violent computer games.

It is also an object to provide a computer system and process of interrupting execution of a computer program according to a set security grade by a user when the computer program contains a security grade which is a program classification code provided by software suppliers for designating an acceptable or unacceptable level of graphic sex, violence, and strong language that exceeds the security grade set by the user.

These and other objects of the present invention can be achieved by a computer system having a function for intercepting lewd/violent programs which includes a central processing unit (CPU) for controlling execution of an application program containing a prede-

Nintendo Exhibit 1003
Part 1 of 2
Page 00439

termined security grade provided by software suppliers; a controller for controlling the direct memory access, and the setting of interruption of the application program; a random-access-memory (RAM) for loading and executing the system and the application program; a read-only-memory (ROM) for storing an initialization program executed when power is turned on, a basic input/output system (BIOS) program for interfacing a hardware and a software, and a security grade setup program; and a security grade memory for storing security grade information to permit execution of the application program and a secret number for identifying the user when changing the security grade information. The central processing unit (CPU) controls the execution of an application program according to the security grade of the application program and the security grade stored in security grade memory, and controls the setting of new security grade and update of security grade memory which limits access of the application program with a different level of graphic sex, violence, and strong language when an input secret number corresponds to a set number of the security grade setup program stored in ROM.

The security grade examination process as contemplated by the present invention includes the steps of comparing the security grade contained in an application program with the security grade set to the computer system, determining whether the security grade set to the computer system enables execution of the present application program, executing the application program when the security grade set to the computer enables execution of the present application program, and outputting the error message when the security grade set to the computer system does not enable execution of the present application program.

The security grade setup process as contemplated by the present invention includes the steps of receiving a secret number when a specific key is input during initialization of the computer system, determining whether the input secret number corresponds to the set secret number, updating a new security grade received by a key input of the user when the two secret numbers coincide with each other, and outputting an error message when the two secret numbers do not coincide with each other.

The present invention is more specifically described in the following paragraphs by reference to the drawings attached only by way of example.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the present invention, and many of the attendant advantages thereof, will become readily apparent as the same becomes better understood by reference to the following detailed description when considered in conjunction with the accompanying drawings in which like reference symbols indicate the same or similar components, wherein:

FIG. 1 is an internal schematic diagram of a typical computer system;

FIG. 2 is an internal schematic diagram of a computer system constructed according to the principles of the present invention;

FIG. 3 is a detailed circuit diagram of a security grade memory of the computer system as shown in FIG. 2;

FIG. 4 is a flow chart illustrating a process of intercepting a lewd/violent program in the computer system according to the principles of the present invention; and

FIG. 5 is a flow chart illustrating a process of inputting the security grade to the computer system according to the principles of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Refering now to the drawings and particularly to FIG. 1, which illustrates a typical computer system such as a personal computer PC. As shown in FIG. 1, the personal computer includes a central processing unit (CPU) 11, a controller 12, a random-access-memory (RAM) 13, a read-only-memory (ROM) 14, a real time clock (RTC) 15, peripheral device controllers 21-26, peripheral device 31-36, and a system bus 38. In particular, the peripheral device controller includes a display controller 21, a keyboard controller 22, a serial interface 23, a parallel interface 24, a floppy disk drive (FDD) controller 25, and a hard disk drive (HDD) controller 26. Likewise, the peripheral device includes a display device 31, a keyboard 32, RS-232C interface 33, a printer 24, a FDD 35, and a HDD 36.

The CPU 11, the controller 12, the RAM 13, the ROM 14, and the RTC 15 are connected with the peripheral device controller 21-26 through the system bus 38, and each peripheral device controller 21-26 is connected to each corresponding peripheral device 31-36. The CPU 11 executes a system program and an application program, and an operation processing function. The controller 12 executes a direct memory access control, a program enable interrupt control and a bus control function. The RAM 13 loads a program executed by the CPU 11, and the ROM 14 stores a power-on self-test (POST) program and a basic input/output system (BIOS) program interfacing of a hardware and a software. The RTC 15 is a timer module having a distinct battery BAT, and has an independent processor for time calculation. In addition, the RTC 15 includes registers in order to memorize the information of the system configuration, and the registers can be substituted the non-volatile memory such as an electrically erasable and programmable read-only-memory (EEPROM) and a

EPODOC ID <EP_ _ _0828209A2 I_>

Nintendo Exhibit 1003
Part 1 of 2
Page 00440

flash memory.

As I have discussed earlier, typical home computer systems such as those in FIG. 1 do not contain any effective provision to prevent teenagers or children from accessing unacceptable application programs that contain an excessive level of violence, nudity, depictions of sexual acts, strong language or other forms of obscenity.

Turning now to FIG. 2 which illustrates a computer system having a function of intercepting lewd/violent programs constructed according to the principles of the present invention. As shown in FIG. 2, the computer system includes a CPU 11, a controller 12, a RAM 13, a ROM 14, a RTC 15, a security grade memory 17, peripheral device controller 21-27, peripheral device 31-37, and a system bus 38.

The peripheral device controller includes a display controller 21, a keyboard controller 22, a serial interface 23, a parallel interface 24, a FDD controller 25, a HDD controller 26 and a CD-ROM interface 27. The peripheral device includes a display device 31, a keyboard 32, a RS-232C interface 33, a printer 24, a FDD 35, a HDD 36 and a CD-ROM drive 37.

The CPU 11, the controller 12, the RAM 13, the ROM 14, the RTC 15 and the security grade memory 17 are connected with each other through the system bus 38, and are connected to the peripheral device controller 21-27. Each peripheral device controller 21-27 are connected to each peripheral device 31-37. The CPU 11 executes the system program and the application program, or the operation processing function. The controller 12 executes the functions of a direct memory access control, a programmable interrupt control and bus control.

RAM 13 loads the program executed by the CPU 11, and the ROM 14 stores an initialization program executed when power is turned on, a basic input/output system (BIOS) program for interfacing a hardware and a software, and a security grade setup program. The RTC 15 is a timer module having a distinct battery BAT, and has an independent processor for time calculation. In addition, the RTC 15 includes registers in order to memorize the information of the system configuration, and the registers can be substituted the nonvolatile memory such as an electrically erasable and programmable read-only-memory (EEPROM) and a flash memory.

Display controller 21 controls a display operation of the display 31, and the keyboard controller 22 controls a key input of the keyboard 32. Also, the keyboard controller 22 can include a logic for interfacing the mouse. The serial interface 23 includes an interface logic for a serial communication, and uses an universal asynchronous receiver/transmitter (UART). The RS-232C interface 33 is an interface device for executing the RS-232C communication method, and is connected to a serial printer, an external modem, a remote personal computer, etc.

Parallel interface 24 is an interface logic for a parallel communication, and a printer 34 connected to the parallel interface is a parallel printer. The FDD controller 25 controls the FDD 35 and connects with at least one FDD. The HDD controller 26 controls the HDD 36 and connects with at least one HDD. The CD-ROM interface 27 controls the access about a CD-ROM between the bus 38 and the CD-ROM drive 37. The security grade memory 17 is used to store a security grade which is a program classification code set by a user for designating an unacceptable level of graphic sex, violence, or strong language contained in different application programs. For instance, after the user sets a predetermined security grade in the security grade memory 17, and if an application program usable in the computer system contains a security grade that either corresponds or exceeds the security grade set by the user in the security grade memory 17, the application program will be interrupted and disabled from operation in order to prevent children from viewing any undesirable content, such as pornography and extreme violence contained in the application program. Alternatively, the security grade memory 17 may be used to store a set of security grade information which are program classification codes individually set by a user for designating different levels of graphic sex, violence, or strong language contained in different application programs. Both embodiments however, require entry of a secret number (password or PIN number) for identifying the user when a new security grade needs to be updated. The data stored by the bus control of the controller 12 is read from the security grade memory 17 and is written into the security grade memory 17 when the application program is executed or the security grade setup program stored to the ROM 14 is executed by the CPU 11.

Now, the reading and writing process of the security grade memory 17 will be explained in detail with reference to FIG. 3 hereinbelow. As shown in FIG. 3, the security grade memory 17 includes an EEPROM 171 and an address decoder 172. The address bus (ADDR[0:10]) is extended from the system bus 38 of the computer system as shown in FIG. 2, and the input port A[0:10] of the EEPROM 171 and the input port of the address decoder 172 are connected to the address bus (ADDR[0:10]). The output port of the address decoder 172 is connected to the chip enable port CE* of the EEPROM 171. The data bus (DATA[0:7]) is extended from the system bus 38 of the computer system as shown in FIG. 2, and is connected to the data input/output port (I/O [0:7]) of the EEPROM 171. A ready/busy (ARDY/BSY) port of the EEPROM 171 is connected to an input/output channel ready (I/O CH-RDY) signal line, and a write enable port WE* and a read enable port RE* are respectively connected to an input/output write IOW* signal line and an input/output read IOR* signal line.

First, a process for reading data stored to the EEPROM 171 will now be described. If the address is generated in order to access the security grade memory while the program of the CPU 11 is executed, the address

Nintendo Exhibit 1003
Part 1 of 2
Page 00441

decoder 172 reads the address input through the address bus (ADDR[0:10]). When the address input through the address decoder 172 corresponds to the EEPROM 171, the address decoder 172 generates a predetermined enable signal and transmits the signal to the chip enable port CEk, and the EEPROM 171 receives the address of the address bus (ADDRFO:101). In addition, the EEPROM 171 outputs a predetermined I/O CH RDY signal through the RDY/BSY port, and the controller 12 generates an input/output read IOR* signal for responding the I/O CH-RDY signal. Accordingly, the EEPROM 171 is in an output enable state, and outputs data corresponding to the input address through the input/output port (I/0[0:7]).

Next, a process for writing the data on the EEPROM 171 will now be described. If the address is generated in order to access the security grade memory while the program of the CPU 11 is executed, the address decoder 172 reads the address input through the address bus (ADDR[0:10]). When the address input through the address decoder 172 corresponds to the EEPROM 171, the address decoder 172 generates a predetermined enable signal and transmits the signal to the chip enable port CE*, and the EEPROM 171 receives the address of the address bus (ADDR[0:10]). Also, the EEPROM 171 outputs a predetermined 1/0 CH-RDY signal through the PDY/BSY port, and the controller 12 generates an input/output write IOW* signal for responding the I/O CH-RDY signal. Accordingly, the EEPROM 171 is in a write enable state, and the data of the data bus (DATA[0:7]) corresponding to the input address is stored through the input/output port (I/0[0:7]).

Security grade memory embodied by an EEPROM is used in the present invention in order to store the security grade, but the technical range of this invention is not limited to this. The security grade information should be maintained even when the power is turned off. As a result, the security grade memory should be a non-volatile memory, and preferably, a flash memory which is part of the ROM 14 and CMOS RAM of the RTC of the computer system as shown in FIG. 2 can be used for storing the security grade. This is because the flash memory in the ROM 14 and the CMOS RAM in the RTC can retain data even when the power is turned off.

A process of controlling interruption of an application program containing a security grade according to a set security grade stored in security grade memory 17 will now be described with reference to FIG. 4 hereinbelow.

First, the CPU 11 initializes an application program when the application program is first inserted into the computer system by way of CD-ROM drive 37 or other available means at step S11. After that, the CPU 11 reads the security grade contained in the application program and the security grade stored in the security grade memory 17 in the manner as described with reference to FIG. 3, and compares the two security grades at S12.

Next, the CPU 11 determines whether the security grade stored in the security grade memory 17 can enable execution of the application program at S13, that is, whether the security grade of the application program does not exceed the security grade of the security grade memory 17. If the security grade of the security grade memory 17 enables execution of the present application program, the CPU 11 executes the application program at step SI4. If the security grade of the security grade memory 17 does not enable execution of the present application program, however, the CPU 11 outputs an error message at step S15. After steps S14 and S15, the CPU 11 terminates execution of the application program at S16.

Different security grades may be stored in security grade memory 17 in order to accommodate different levels of violence, vulgarity and lewdness of different application programs. The users may need to adjust or set different security grade. For example, the security grade needs to be changed when the user is changed from teenagers to adults.

A process of changing new security grade in the security grade memory 17 will now be described as follows. When the user inputs a specific key on booting the computer system, the security grade setup program stored to the ROM 14 is executed at step S21. And, the user inputs a secret number by a key input at step S22. The CPU 11 determines whether the secret number input by the user at step S22 corresponds to the secret number set to the security grade memory 17. If the secret number input by user at step S22 corresponds to the set secret number of the security grade memory 17, the user inputs a new security grade by the key input at step S24, and if not so, the CPU 11 outputs the error message at step S25. After steps S24 and S25, the setup program is terminated at step S26, and the CPU 11 executes a next routine.

As described above, the computer system according to the principles of the present invention has an internal memory for storing a security grade which is a program classification code set by a user for designating an unacceptable level of graphic sex, violence, or strong language contained in an application program. Accordingly, when an application program containing a security grade that exceeds the security grade stored in the internal memory is inserted into the computer system, no execution of that application program is permitted. As a result, the computer system constructed according to the principles of the present invention can effectively stop teenagers from executing application program that contains an unacceptable level of graphic sex, violence or strong language.

While there have been illustrated and described what are considered to be preferred embodiments of the present invention, it will be understood by those skilled in the art that various changes and modifications may be made, and equivalents may be substituted for elements thereof without departing from the true scope

BNSDOCID <EP_____ 0828209A2 I >

Nintendo Exhibit 1003
Part 1 of 2
Page 00442

of the present invention. For example, if the computer system is further constructed to serve as a television receiver, then the application program can also encompass television programs that carry different program classification codes for different levels of graphic sex, violence and strong language. In addition, many modifications may be made to adapt a particular situation to the teaching of the present invention without departing from the central scope thereof. Therefore, it is intended that the present invention not be limited to the particular embodiment disclosed as the best mode contemplated for carrying out the present invention, but that the present invention includes all embodiments falling within the scope of the appended claims.

Claims

1. A computer system, comprising:

   a first memory device for storing an initialization program and a security grade setup program;
   a second memory device for storing a security grade which is a program classification code selected by a user for designating an unacceptable program content contained in an application program, and a password for identifying the user when changing the security grade; and
   a controller for controlling execution of an application program according to the security grade of the application program and the security grade stored in said second memory device during operation of said initialization program, and for controlling the changing of the security grade stored in said second memory device during operation of said security grade setup program, when the user inputs a password that corresponds to the password stored in said second memory device.

2. The computes system of claim 1, further comprised of said first memory device corresponding to a read-only-memory.

3. The computer system of claim 1, further comprised of said second memory device corresponding to a non-volatile memory.

4. The computer system of claim 1, further comprised of said second memory device comprising:

   an electrically erasable and programmable read-only-memory having an address port and a data port respectively connected to corresponding signal lines of a system bus, for executing data read/write operation under control of said controller; and
   an address decoder for reading address input through the address port of said electrically erasable and programmable read-only-memory, and determining whether an input address corresponds to said electrically erasable and programmable read-only-memory.

5. A method for controlling a computer system having a function of interrupting lewd/violent programs, said method comprising the steps of:

   receiving an application program in the computer system;
   comparing a security grade contained in an application program with a security grade set in the computer system when the application program is executed;
   determining whether the security grade set in the computer system enables execution of the application program;
   executing the application program when the security grade set in the computer system enables execution of the application program; and
   alternatively, providing a visual display of an error message indicating that the application program cannot be executed, when the security grade set in the computer system does not enable execution of the application program.

6. The method of claim 5, further comprised of the security grade set in the computer system enabling execution of the application program, when the security grade contained in the application program exceeds the security grade set in the computer system.

7. The method of claim 5, further comprising:

   receiving a password when an user inputs a specific key via a key input unit designating said password during initialization of the computer system;
   determining whether the password input by the user corresponds to a set password; and
   updating a new security grade, via said key input unit, when the password input by the user corresponds to the set password; and
   alternatively, providing a visual display of an error message when the password input by the user does not correspond to the set password

8. The method of claim 6, further comprising:

   receiving a password when an user inputs a specific key via a key input unit designating said password during initialization of the computer system;
   determining whether the password input by the

Nintendo Exhibit 1003
Part 1 of 2
Page 00443

user corresponds to a set password; and

updating a new security grade, via said key input unit, when the password input by the user corresponds to the set password; and

alternatively, providing a visual display of an error message when the password input by the user does not correspond to the set password.

9. A computer system, comprising:

a central processing unit;

a first memory for loading a program executed by the central processing unit;

a second memory for storing an initialization program and a security grade setup program;

a security grade memory device for storing a security grade which is a program classification code selected by a user for designating an unacceptable program content contained in an application program, and a password for identifying the user when changing the security grade;

a plurality of peripheral device controllers for driving operation of a plurality of peripheral devices including a display device, a keyboard, a printer, a hard disk drive and a compact-disk-read-only-memory drive; and

said central processing unit controlling execution of an application program according to the security grade of an application program and the security grade stored in said security grade memory device during initialization, and for controlling the changing of the security grade stored in said security grade memory device during said security grade setup, when the user inputs a password that corresponds to the password stored in said security grade memory device.

10. The computer system of claim 9, further comprised of said first memory corresponding to a random-access-memory.

11. The computer system of claim 9, further comprised of said second memory corresponding to a read-only-memory.

12. The computer system of claim 9, further comprised of said security grade memory device corresponding to a non-volatile memory.

13. The computer system of claim 9, further comprised of said security grade memory device comprising:

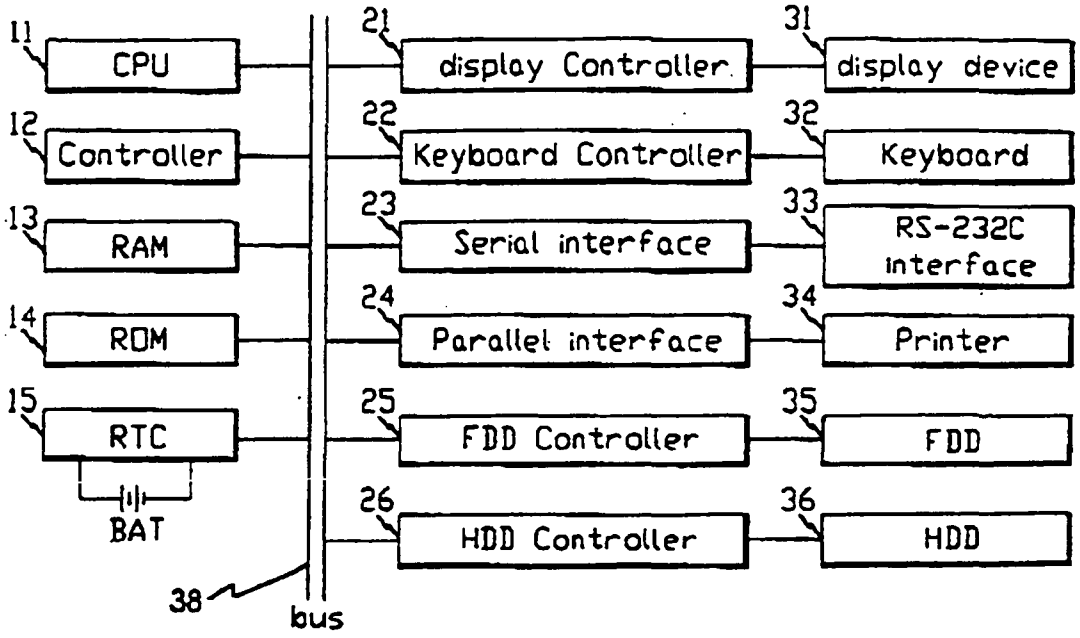
an electrically erasable and programmable read-only-memory having an address port and a data port respectively connected to corresponding signal lines of a system bus, for executing data read/write operation; and

an address decoder for reading address input through the address port of said electrically erasable and programmable read-only-memory, and determining whether an input address corresponds to said electrically erasable and programmable read-only-memory.

EPNSDOCID <EP 0828209A2 I >

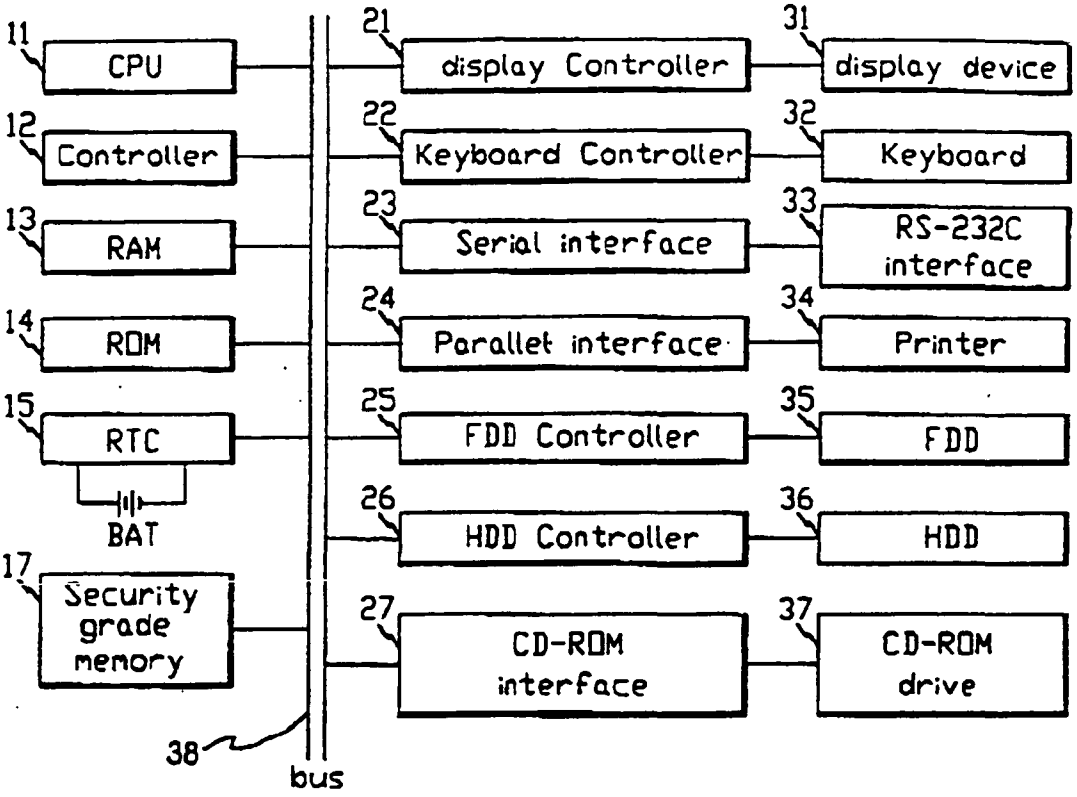
Nintendo Exhibit 1003
Part 1 of 2
Page 00444

FIG.1



Nintendo Exhibit 1003
Part 1 of 2
Page 00445

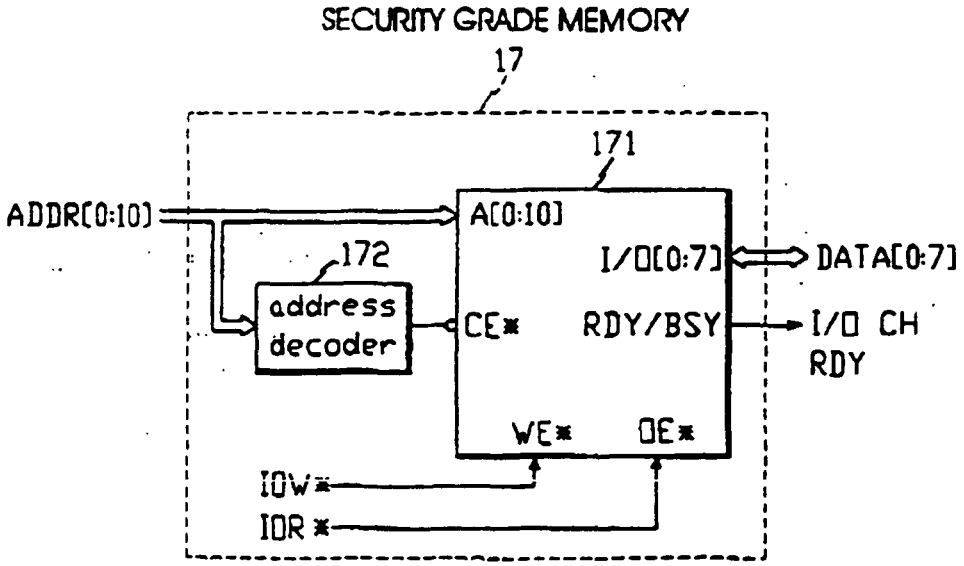
FIG.2



BNSDOCID <EP. __ __0828209A2 I >

Nintendo Exhibit 1003
Part 1 of 2
Page 00446

FIG.3



Nintendo Exhibit 1003
Part 1 of 2
Page 00447

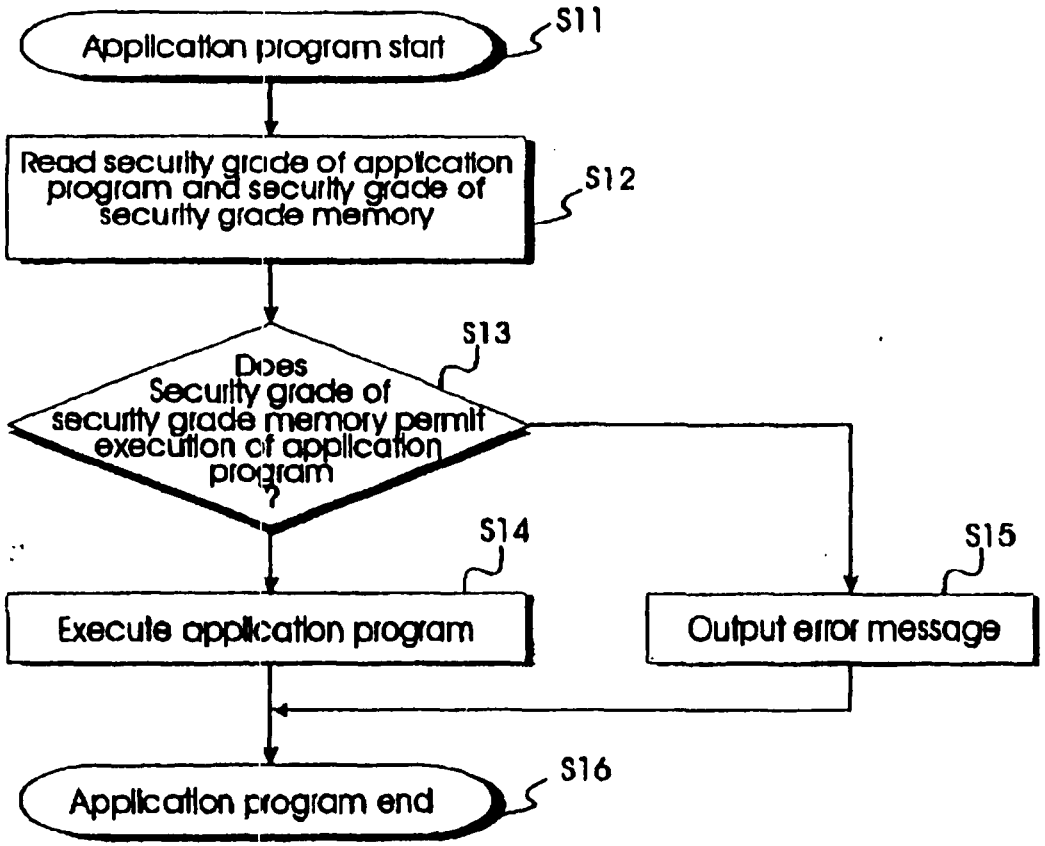


FIG. 4

Nintendo Exhibit 1003
Part 1 of 2
Page 00448

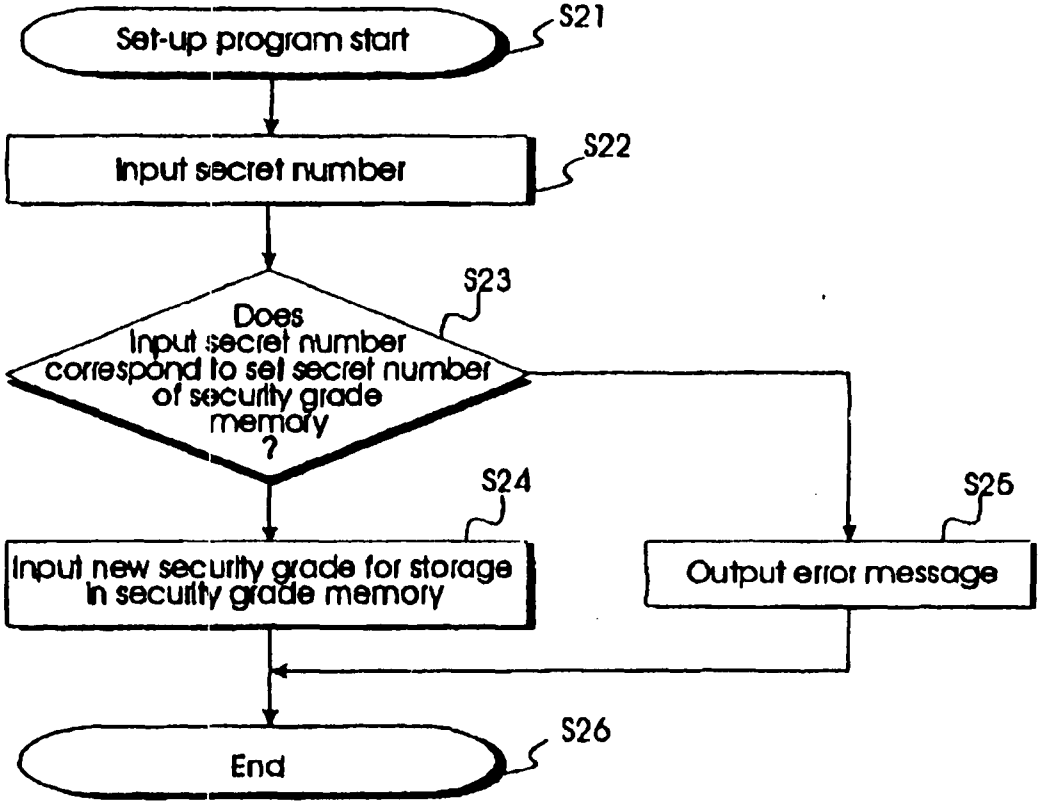


FIG. 5

Nintendo Exhibit 1003
Part 1 of 2
Page 00449

(12) UK Patent Application (19) GB (11) 2 378 780 (13) A

(43) Date of A Publication 19.02.2003

(21) Application No 0119846.4

(22) Date of Filing 14.08.2001

(71) Applicant(s)
Elan Digital Systems Limited
(Incorporated in the United Kingdom)
Elan House, Little Park Farm Road,
Segensworth West, FAREHAM,
Hampshire, PO15 5SJ, United Kingdom

(72) Inventor(s)
Kevin Wemyss
Anthony Feliks Olech

(74) Agent and/or Address for Service
D Young & Co
21 New Fetter Lane, LONDON, EC4A 1DA,
United Kingdom

(51) INT CL[7]
G06F 17/60

(52) UK CL (Edition V)
G4A AAP

(56) Documents Cited
EP 1056010 A1
EP 1030237 A1
WO 1995/015522 A1
WO 2000/048063 A1
WO 1999/027475 A1
US 5944821 A
US 5930777 A
US 5619571 A
US 5421006 A

(58) Field of Search
UK CL (Edition T) G4A AAP
INT CL[7] G06F 1/00 12/14 17/60
Other: ONLINE:WPI,EPODOC,JAPIO

(54) Abstract Title
An arrangement for preventing the re-use of tokens in accessing pay-per-use software

(57) A method for consuming tokens used to control access to restricted resources held at a user's machine (106) is disclosed. The method comprises: reading a stored token from a first storage area of the user's machine (106), calculating control information for verifying the integrity of the stored token, reading predetermined control information corresponding to the stored token from a second storage area, comparing the control information to the predetermined control information; and consuming the stored token conditional on the control information matching the predetermined control information. The first and second storage areas are separate to help reduce the vulnerability of the tokens to selective replay attack.

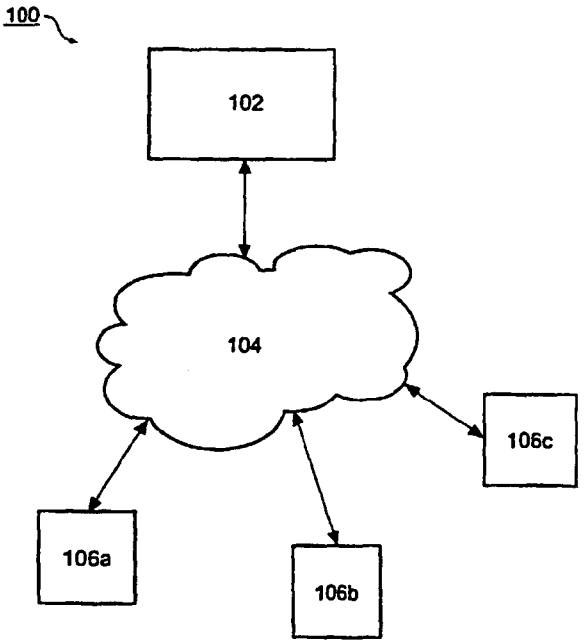


Fig. 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

GB 2 378 780 A

BNSDOCID: <GB_____2378780A__I_>

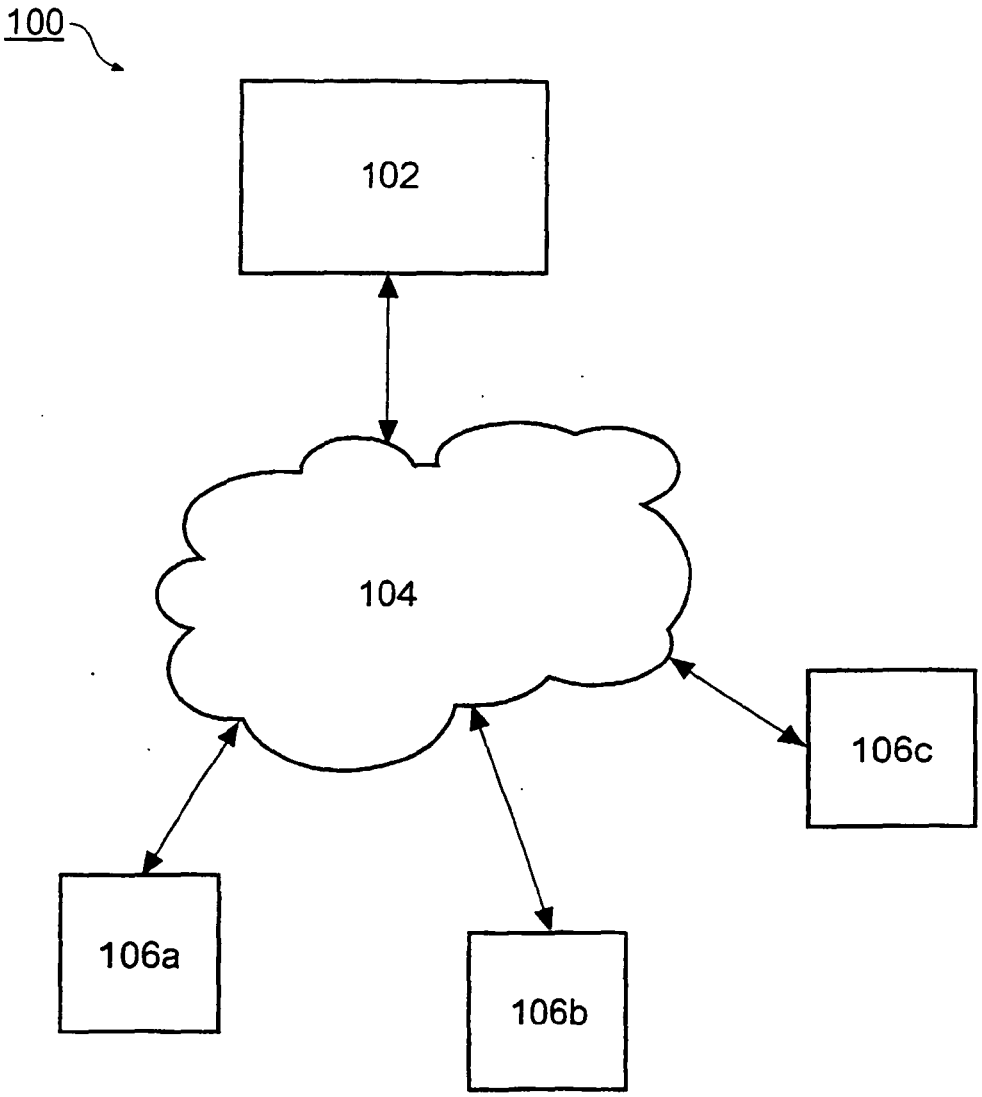


Fig. 1

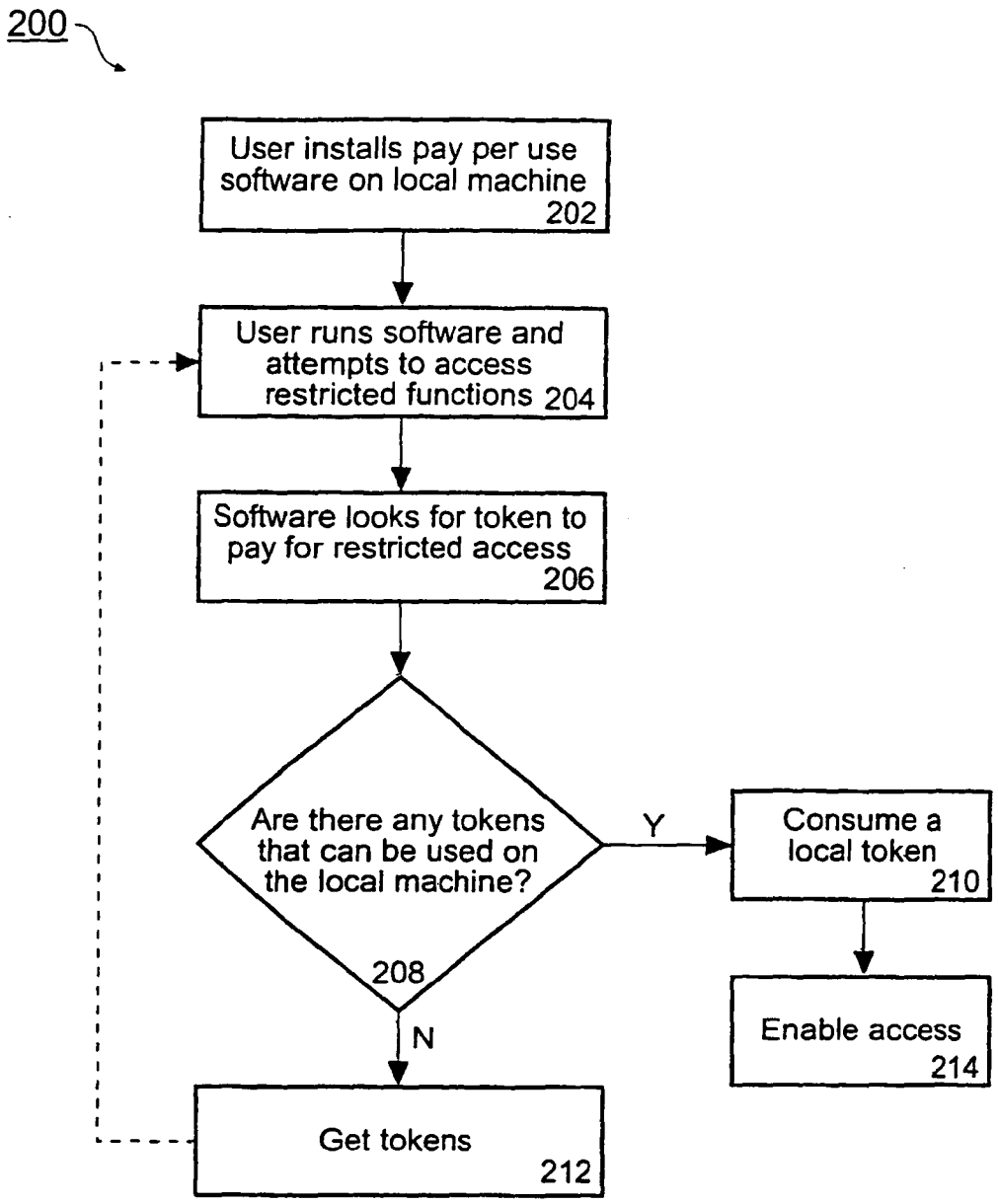


Fig. 2

BNSDOCID: <GB 2378780A_I >

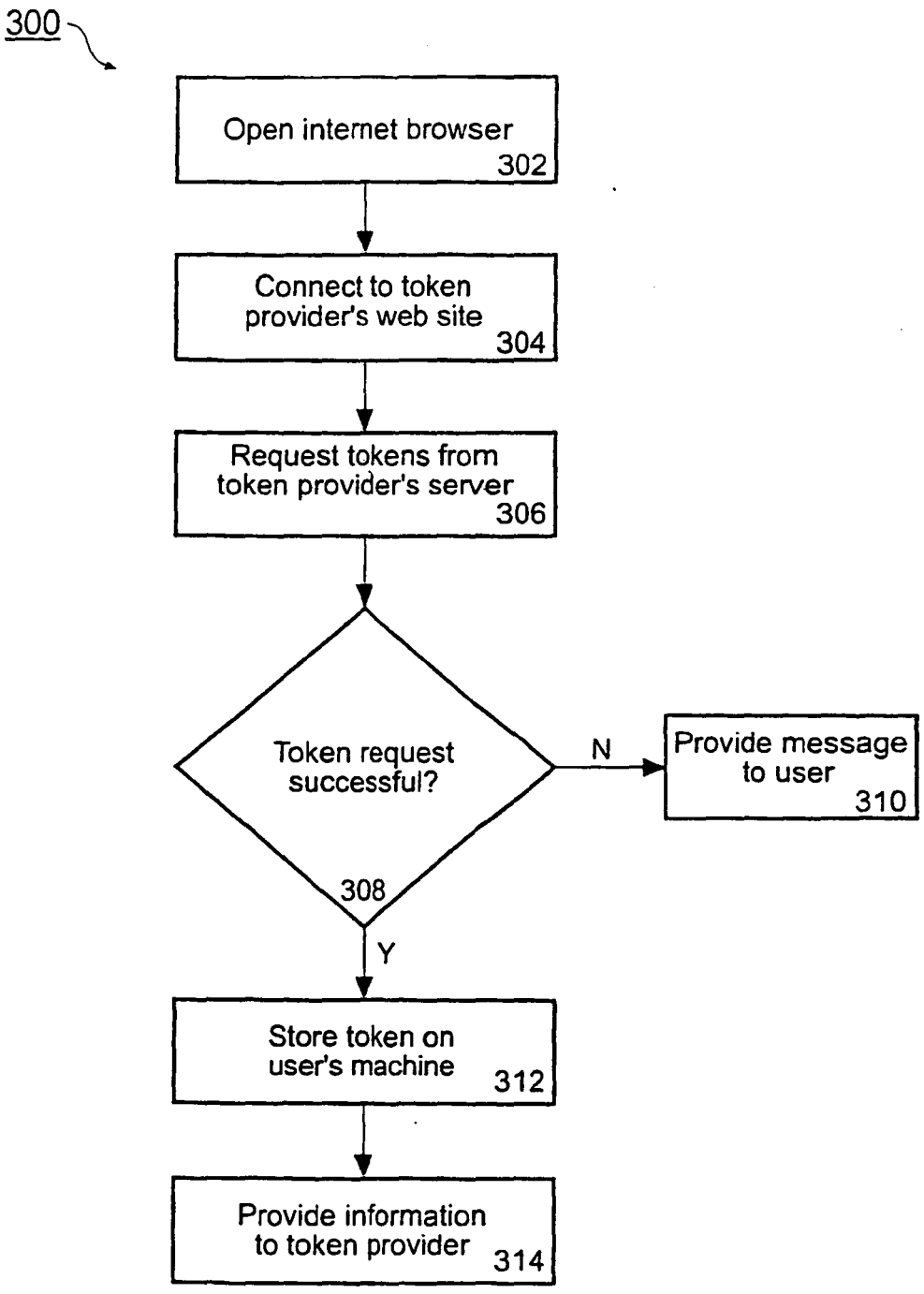

300
Open internet browser
302
Connect to token provider's web site
304
Request tokens from token provider's server
306
Token request successful?
308
N
Provide message to user
310
Y
Store token on user's machine
312
Provide information to token provider
314

Fig. 3

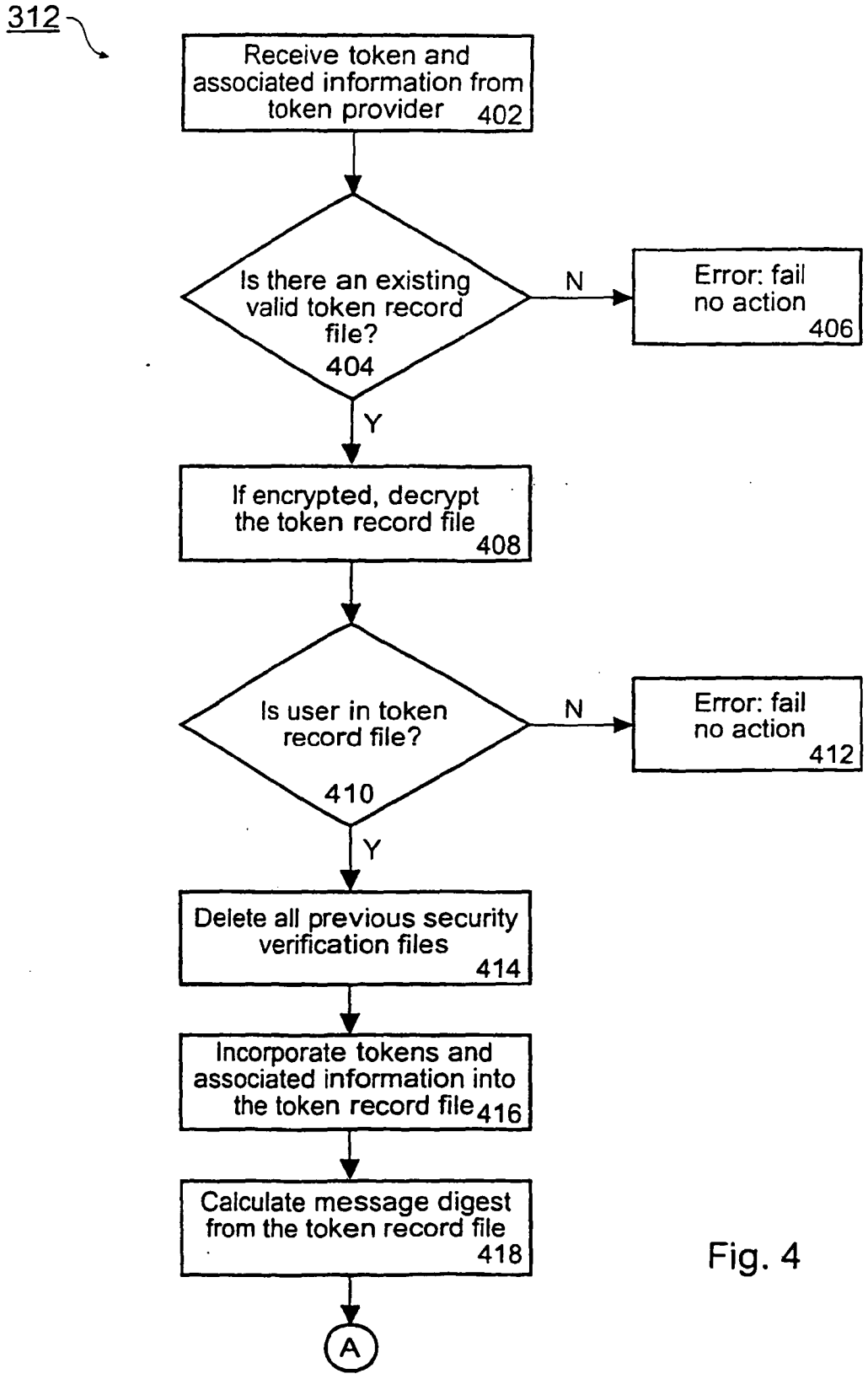


Fig. 4

BNSDOCID: <GB_____2378780A_I_>

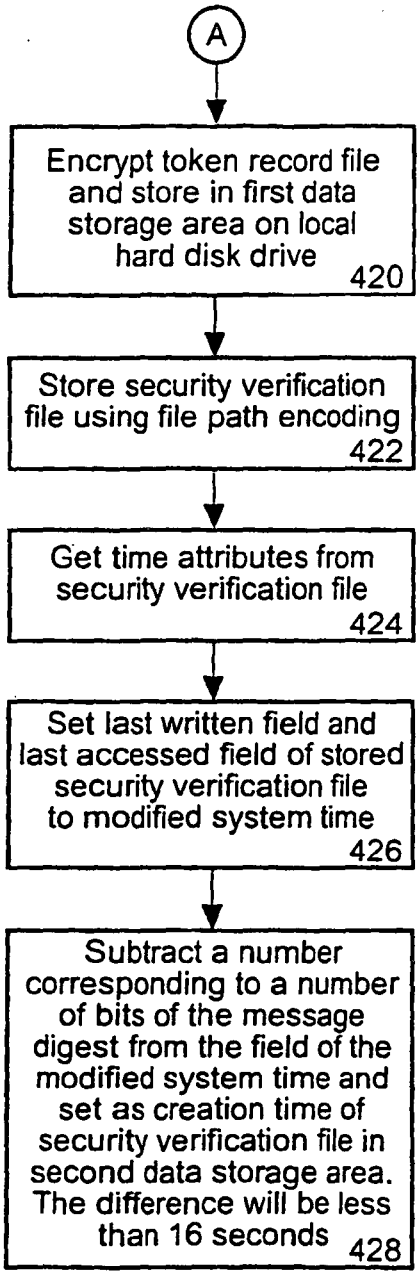

A
Encrypt token record file and store in first data storage area on local hard disk drive
420
Store security verification file using file path encoding
422
Get time attributes from security verification file
424
Set last written field and last accessed field of stored security verification file to modified system time
426
Subtract a number corresponding to a number of bits of the message digest from the field of the modified system time and set as creation time of security verification file in second data storage area. The difference will be less than 16 seconds
428

Fig. 5

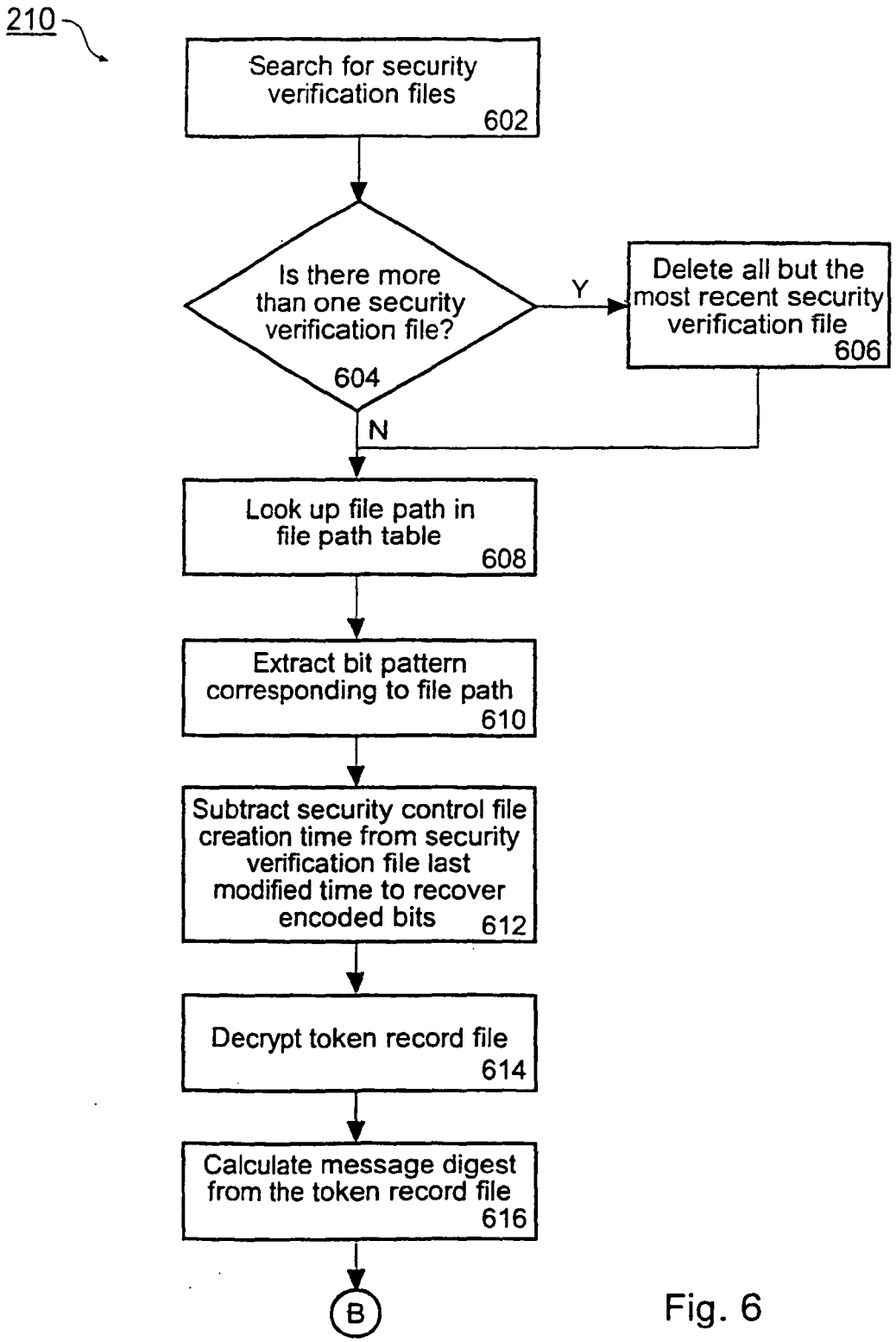


Fig. 6

BNSDOCID: <GB_____2378780A__I_>

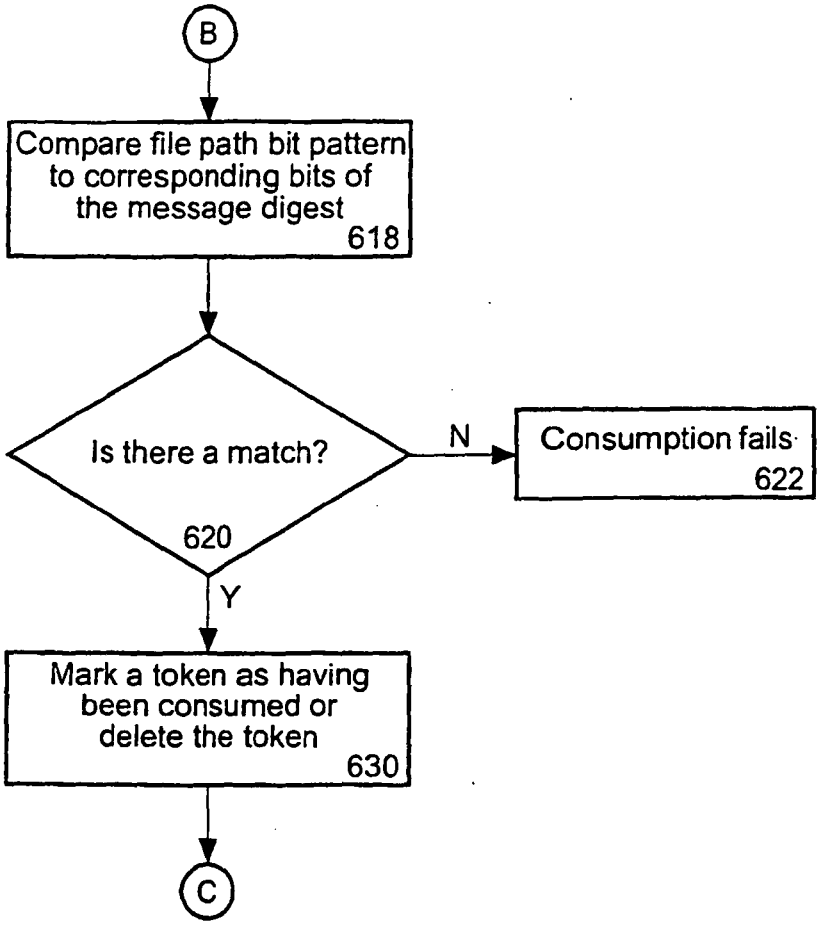

B
Compare file path bit pattern to corresponding bits of the message digest
618
Is there a match?
620
N
Consumption fails
622
Y
Mark a token as having been consumed or delete the token
630
C

Fig. 7

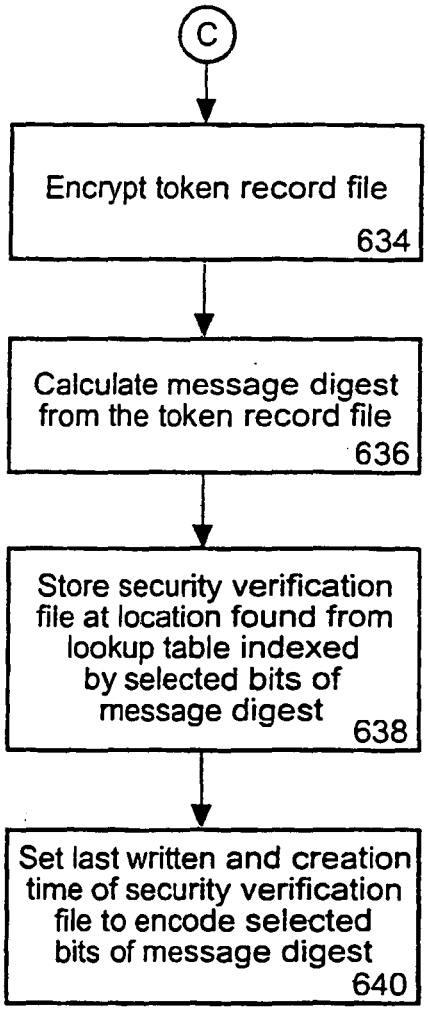


Fig. 8

BNSDOCID: <GB_____2378780A_1_>

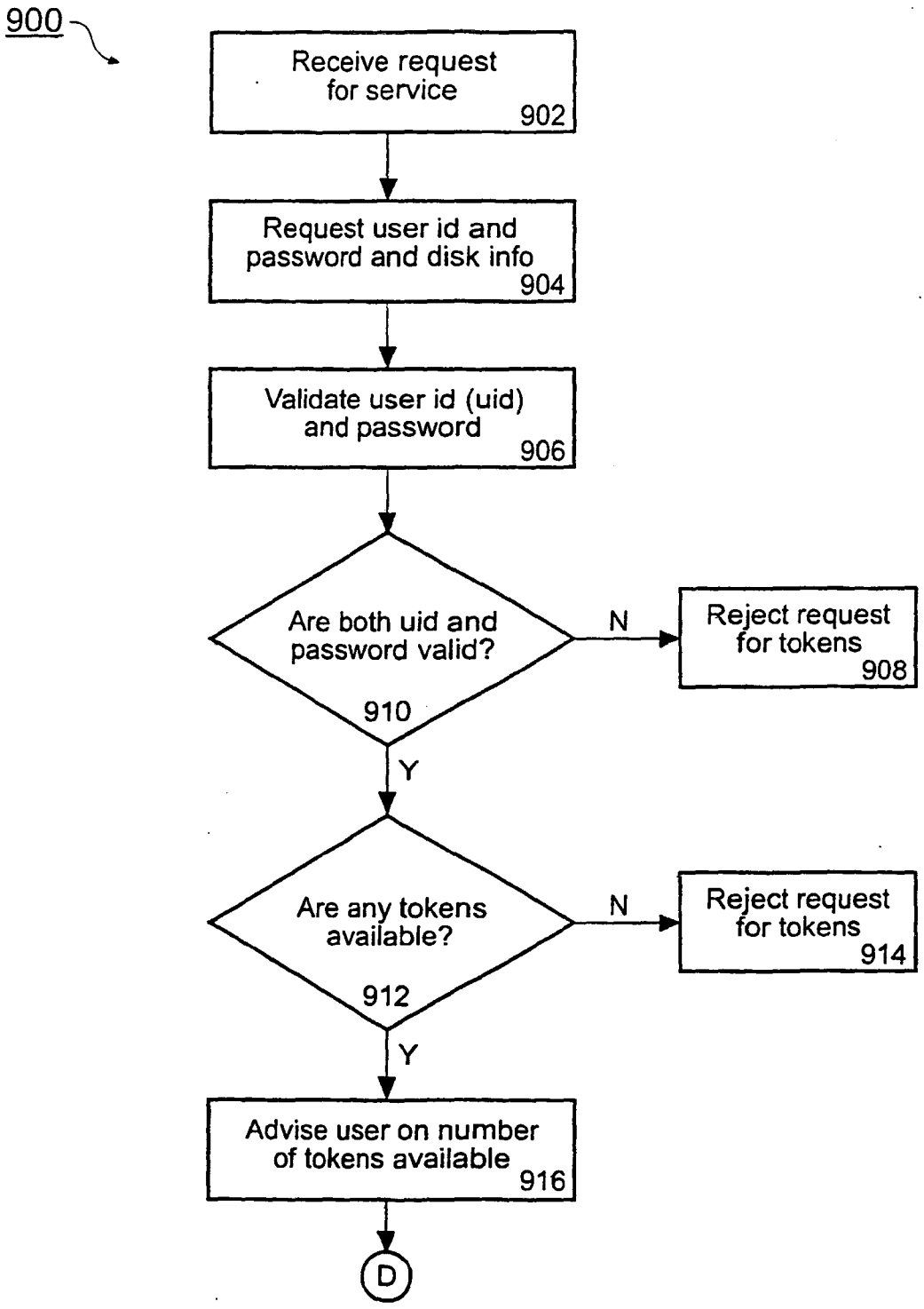

900
Receive request for service
902
Request user id and password and disk info
904
Validate user id (uid) and password
906
Are both uid and password valid?
910
N
Reject request for tokens
908
Y
Are any tokens available?
912
N
Reject request for tokens
914
Y
Advise user on number of tokens available
916
D

Fig. 9

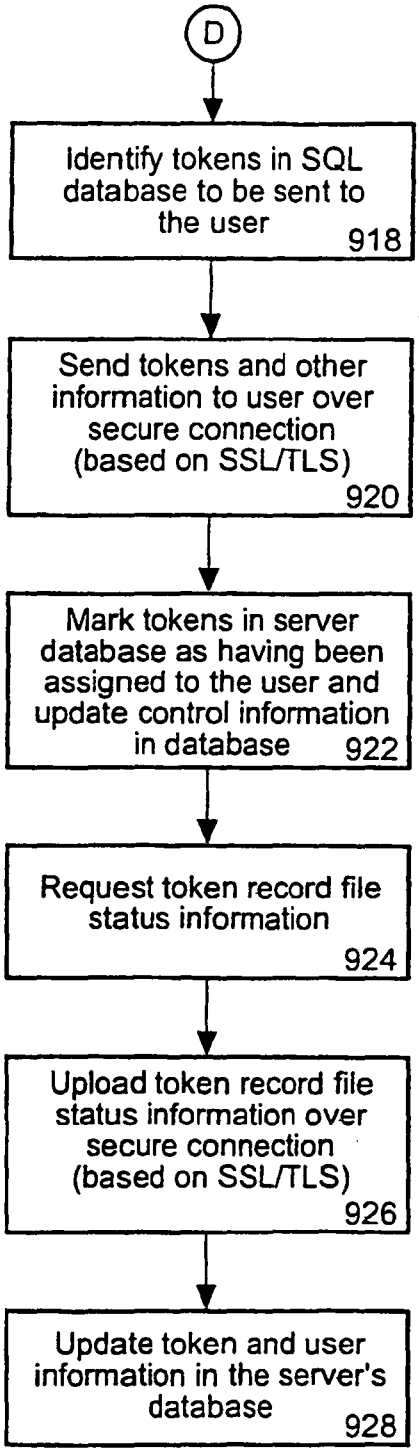


Fig. 10

BNSDOCID: <GB_____2378780A__I_>

Title of the Invention

Data integrity

Background of the Invention

The present invention relates to data integrity. In particular it relates to ensuring the integrity of stored data so that any tampering with the stored data is detectable.

Data integrity is important for many applications. It is particularly important where the data is commercially valuable, such as where the data itself has intrinsic value, where the data represents a financial sum or transaction, or where the data acts as a means for enabling access to useful or valuable resources. One example of the latter such case arises where data tokens are used to control access to resources over networks. The tokens may be used to control access to pay-per-access or pay-per-view resources that are conditionally accessible from, for example, the Internet. These tokens are therefore more valuable than a mere collection of data values, in that they also represent monetary value. Thus, the integrity of such tokens is important in preventing fraud and ensuring just revenue for the provider of the resources.

Several schemes exist to reduce the likelihood of fraudulent use of tokens in e-commerce systems such as the pay-per-access or pay-per-view systems previously mentioned. Often tokens are exchanged between vendors and customers when connected over a communications link, such as when a customer connects to a vendor's internet-based web-site. Typically, the exchange of tokens will require the intervention of a third party at some stage of proceedings to confirm that payment will be, or has already been, made for the tokens. However, both direct on-line exchange of tokens between a customer and vendor and on-line verification of tokens involving third party intervention are inconvenient where rapid access to token-consuming resources is required. Such systems are also inconvenient where resources are to be accessed from remote locations where communications links may not be readily available or may only operate at slow data transfer rates.

An example of the inconvenience of prior art systems is perhaps best illustrated by considering the following example situation. Personnel working "in the field",

such as engineers repairing photocopying or computer equipment at client sites, often require access to software applications, such as, for example, diagnostic software tools. Such applications are increasingly licensed for use on a pay-per-use basis. The licence may require the licensee to pay a fee whenever the application is used successfully to complete a job, as indicated by saving a log-file to the engineer's laptop computer hard disk, or following the printing of an invoice or record for the client, for example. The engineer will typically visit many sites in any one day and may use software applications that are traditionally accessed from his local hard disk drive many times per day. This creates a difficulty for the licensor of the software applications when it comes to calculating the fee due for use of those applications.

One solution to this problem of monitoring use of software applications has been to require the engineer to connect his portable machine to a server belonging to the licensor to request access. Typically, the licensor's server verifies the engineer's credentials and either takes an immediate payment or deducts payment from an account which the engineer is authorised to use whilst the engineer's laptop is connected. This scheme has numerous disadvantages which inconvenience the engineer, in particular. Engineers often have to move between numerous client sites and may have to carry additional communications equipment to connect their portable devices, such as laptop computers, to the licensor's server. Additionally, forcing the engineer to access the licensor's server every time access to token-consuming resources is needed is time consuming, repetitive and can be frustrating for the engineer when the infrastructure of the site at which he is working only permits a low-speed access, or worse still has no access, to the licensor's server.

An example of a prior art system that requires on-line verification for permitting access to network resources, in this case pay-per-view world wide web pages, is described in US-A-5,930,777. In the system described in US-A-5,930,777 a first party requiring access to a vendor's pay-per-view web pages is directed to a third party, called a banker, that acts as an intermediary between the first party and the vendor. The banker mints tokens and routes the first party to the pay-per-access web pages. The vendor is then credited for the accessed pages without the user learning the network location of the vendor's pay-per-access pages.

Nintendo Exhibit 1003
Part 1 of 2
Page 00462

Other types of prior art system exist to control access to resources held in data processing systems. For example, it is known to use hardware devices connected to computer systems to ensure that access to software resources is permitted only on a single machine in exchange for appropriate payment. One example of such a system that can be used to control pay-per-access or pay-per-view to resources includes a so called smart card reader that can be used to deduct payments from a securely encrypted card comprising a microprocessor device. Although reasonably secure, such systems are generally recognised as being inconvenient and expensive due to the necessary extra hardware that needs to be added to existing computer systems.

Another way of controlling access to pay-per-use or access systems is to store non-reconciled tokens locally on a computer system that can then consume those tokens as and when necessary. Additional tokens can then be purchased and may be loaded onto the computer system either via a network, or perhaps by a token-provider sending a machine readable medium to the system operator. Such systems rely heavily on the honesty of the user to pay for all the tokens he consumes because it is relatively easy for the user merely to copy existing token record files, use the resources and then selectively re-install the token record files containing credits he has already spent, particularly where the vendor has no way to reconcile the use of the tokens with his records. This method of fraudulently re-installing token record files following previous consumption of the tokens is known as a selective replay attack.

Due to the ease of performing selective replay attacks, the preferred technique for permitting access to pay-per-use resources, particularly resources such as valuable applications such as software used by field engineers, remains to use either an on-line verification technique and/or a hardware device and consequently to tolerate the inherent disadvantages associated with such techniques as described above.

Summary of the Invention

According to a first aspect of the present invention there is provided a method for consuming non-reconciled tokens. the method comprising: reading a stored token from a first storage area; calculating control information corresponding to the stored token; reading predetermined control information corresponding to the stored token from a second storage area, wherein the first storage area is separate from the second storage area; comparing the control information to the predetermined control information; and consuming the stored token conditional on the control information matching the predetermined control information. The separation of token data from separate control information prevents opportunist selective replay attacks as both sets of information are needed to consume tokens. Preferably the control information can be hidden from any user and/or at least partially encoded so that it is not immediately evident to the user which information he needs to copy and to where in order to have access to resources.

The resources, for which access is controlled in exchange for consumption of tokens, may be software such as an application program and/or hardware use such as printer, processor, disk drive, memory or communications resources, for example. The resources may be located remotely from any data processing apparatus used to access them, for instance by way of access over a network or by supplying them on removable media, or may be located at the data processing apparatus. The data processing apparatus can be a portable machine for ease of mobility, such as, for example, a laptop computer, a PDA, or a WAP-enabled mobile telephone device, although it may also be any other type of data processing apparatus.

The first and second storage areas can be located on the same type of storage medium or may be found in different media. By way of non-limiting example, the storage areas can be located on or in any one or combination of: memory, flash memory, hard disk storage space, FDD storage space etc., and they may additionally be located separately on different devices on a network. According to one further aspect of the invention the first and/or second data storage areas can be encrypted to further reduce the likelihood of tampering by users.

According to another aspect of the invention, tokens bought by the user are stored in a token record file. The token record file can be used as a "wrapper" into which further tokens and additional information regarding the tokens themselves, the user, the user's machine, validity information etc. can be added. Information regarding the token record file (such as, for example, user privileges that determine whether a user is to be given credit when buying tokens, how many tokens they are allowed to have, the maximum token value they can use in a particular time etc.) may be stored by a token provider, such as at a token provider's server. In this way it is possible that when a user working for a company wants to download tokens he can be prevented from downloading his entire company's allocation to a single machine and hogging all the tokens to the detriment of his colleagues.

The token record file may be used to keep a record of token usage on a portable machine that may be uploaded at a later time to a token provider's server. This record may be used to determine the amount due for pay-per-use resources at a date sometime after the tokens used to access the pay-per-use resources have been consumed. In this way customers of the token provider may be provided with credit facilities. The record may also indicate that certain tokens have time-expired and/or may be used to record indicators of any suspicious activity that have taken place on the user's machine in order to detect possible fraudulent activity. Consumption of tokens may be permitted conditional on a user connecting to a token provider's server within a predetermined time period. This helps ensure that users contact the token provider regularly, thereby allowing the token provider to supply them with software updates and special offers etc., and to check for any suspicious user activity. To this end, an interval timer may be used at the user's data processing apparatus. The interval timer may be reset every time a user connects to the token provider's server.

According to one further aspect of the invention, the control information corresponding to the stored token is calculated from the token record file using, for example, a message digest. However, any form of encoding, checksumming, hashing and/or encryption algorithm could be used to create the control information provided it gives a reproducible code sequence output when operating on the same input data. The control information may be calculated using only the data in the token record file, or it may also use other information specific to a particular data processing apparatus,

such as. for example, a processor serial number and/or a hard disk drive serial number. This can help prevent selective replay attacks and can help ensure that token use can be localised to the particular apparatus for which the tokens are distributed by the token provider.

According to another aspect of the invention at least one security verification file may be stored in the second storage area. The security verification file(s) may be used to contain and/or encode control information relating to stored tokens. The second storage area(s) may be selected from among a plurality of such areas. The security verification file, or files, may store arbitrary data and/or at least part of the control information as content.

According to another aspect of the invention a method for consuming the stored tokens is provided. The method of consuming the tokens may entail modifying the token record file by marking a token contained therein as having been used. A modified token record file containing the token marked as used can then be used to overwrite the previous token record file. New predetermined control information can be calculated from the new token record file written to the second storage area. The new control information may be written in one or more security verification files. The previous control information may be deleted. In this way the token record file and associated control information can be automatically updated to reflect changes to either the tokens and/or the additional information stored in the token record file. In a further aspect of the invention, a check is made for the presence of a plurality of token record files and/or security verification files, and all except the most recent can be deleted. This not only ensures "good housekeeping" of the storage areas, but also helps to frustrate selective replay attacks.

According to yet another aspect of the invention data corresponding to at least part of the control information may be hidden using a steganographic hiding technique. Steganographic techniques can be used to help prevent the user being aware that control information exists and/or how it relates to the information contained in the token record file. Any suitable steganographic technique can be used. For example, one or more bits of information corresponding to part, or the whole, of the control information can be hidden by encoding them in file date/time information and/or file path information.

According to an aspect of the invention there is provided a method for storing consumable non-reconciled tokens, the method comprising: receiving a token from a token provider; storing the token in a first storage area; obtaining predetermined control information corresponding to the token; and storing the predetermined control information in a second storage area, wherein the first storage area is separate from the second storage area. The first and second storage areas may be contiguous. The predetermined control information may be determined either by the token provider, or could be calculated by a data processing apparatus located remotely from the token provider. In the former case, the predetermined control information may be downloaded to the user's data processing apparatus. The token provider can be a server, and may provide a service to the user's machine by way of an Internet connection using a world wide web interface. According to another aspect of the invention a check is made for the presence of any token record files and/or security verification files, and if none are found an error may be reported. Any token record files and/or security verification files except the most recent can then be deleted.

Yet another aspect of the invention relates to a method for supplying consumable non-reconciled tokens, the method comprising: generating a unique token; storing a copy of the unique token in at least one data storage device; and providing the unique token to a data processing apparatus for storage in a first storage area, wherein the data processing apparatus is operable to store predetermined control information corresponding to the unique token in a second storage area separate from the first storage area. The method may additionally comprise supplying any desired information to the user's data processing apparatus.

In order to manage the token record file according to a further aspect of the invention, a token supplier, or the user's data processing apparatus, may read an expiry time from the token record file (or elsewhere), compare the expiry time to a current system time and refuse to work with the tokens until the expiry time is updated. The expiry time may be calculated as a time interval since a last update. The expiry time may be calculated by way of an interval timer that operates at the user's data processing apparatus. Updating of the expiry time may involve connection to the token provider's server.

According to another aspect of the invention data indicating the number of used tokens and/or unused tokens may be stored at the user's data processing apparatus and/or may be stored on a token provider's server. Tracking the number of tokens and their various statuses allows the token provider the possibility of monitoring a multitude of statistical information (such as a user's rate of token consumption, for example) that can be used to indicate possible fraud and/or provide a tailored service to customers. Events, such as special offers, requests for information etc. may be triggered conditional on the statistical information gathered. For example, triggers may include the numbers of tokens having a particular status being lower than, equal to or higher than various thresholds and/or other triggering criteria, such as rate may be used.

By reading the predetermined control information from the data processing apparatus, reading the unique token from the data processing apparatus, calculating control information from the copy of the unique token, and comparing the predetermined control information to the calculated control information to determine whether there is a match, another aspect of the invention may check for fraudulent activity. If fraudulent activity is detected or suspected, the token provider may refuse to supply further tokens to a particular user, may withdraw credit facilities, may query the user and/or may invalidate existing tokens at the user's data processing apparatus at the earliest opportunity. Many varied actions are possible in response to confirmed user fraud.

According to another aspect of the invention the token provider, or providers, may detect whether resources at the user's data processing apparatus or elsewhere are up-to-date and if not may supply an update, possibly during the same session in which tokens are provided for the user's use.

According to another aspect of the invention any part, including the whole, of any of the methods described herein is/are implemented as a computer program that configures a data processing apparatus to implement that method or partial method. The computer program(s) may comprise a module or plug-in, or a set of modules or plug-ins, that are operable to configure a web-browser or web-browsers located on one or more data processing apparatus to implement, either individually or together, any aspect of the methods of the present invention.

In a further aspect of the invention, there is provided a carrier medium for the previously described computer program(s). The carrier medium may comprise a magnetic storage medium such as a tape or disc storage medium, an optical storage medium such as a read/write, CD-ROM or solid-state memory. Such storage media may be delivered to a user for loading onto a suitable data processing apparatus. Optionally, the carrier medium may comprise a telecommunications carrier medium, the computer program(s) being embodied as an electronic or electrical signal carried by the telecommunications signal. Such a carrier medium may be an RF carrier signal, or an optical carrier signal for an electronic carrier signal.

In yet another aspect of the present invention, there is provided a data processing apparatus for providing access to resources in exchange for consumption of a consumable non-reconciled token, the data processing apparatus comprising: a controller operable to access at least one data storage device, wherein the at least one data storage device is configured to provide at least a first and a separate second storage area, wherein the first storage area contains data encoding a stored token and the second storage area contains data encoding predetermined control information corresponding to the stored token; and a processor configured to: read the stored token from the first storage area; calculate control information corresponding to the stored token; read predetermined control information corresponding to the stored token from the second storage area; compare the control information to the predetermined control information; and permit access to resources and consume the stored token conditional on the control information matching the predetermined control information. If the token is stored in a token record file in an encrypted form in the first storage area, the token may be decrypted and the token extracted.

According to a further aspect of the invention, there is provided a data processing apparatus for generating and distributing consumable non-reconciled tokens, the data processing apparatus comprising: a communications interface; at least one data storage device; and a processor configured to: generate a unique token; store a copy of the unique token in the at least one data storage device; and provide the unique token via the communications interface to a further data processing apparatus for storage in a first storage area, wherein the data processing apparatus is operable to

store predetermined control information corresponding to the unique token in a second storage area separate from the first storage area.

According to yet another aspect of the invention. there is provided a method for hiding data, comprising: generating a digital fingerprint from a data file stored in a first storage area; and hiding the digital fingerprint by storing at least part of the digital fingerprint in a second storage area, wherein the first storage area is separate from the second storage area. Optionally, the second storage area may not be directly accessible to a user. The method may comprise generating the digital fingerprint from a message digest generated using the data file. At least part of the digital fingerprint may be hidden using a steganographic technique. The steganographic technique may comprise encoding at least one bit of the digital fingerprint by storing a security verification file at a predetermined file location selected from a plurality of such predetermined file locations. The steganographic technique may comprise encoding at least one bit of the digital fingerprint by modifying a file time stamp of a, or the, security verification file.

BNSDOCID: <GB_____2378780A_I_>

Brief Description of the Drawings

For a better understanding of the invention and to show how the same may be carried into effect reference is now made by way of example to the accompanying drawings in which:

Figure 1 shows a system in which a plurality of data processing apparatus for providing access to resources in exchange for consumption of a token according to one aspect of the invention are connected via a network to a data processing apparatus for generating and distributing tokens according to another aspect of the invention.

Figure 2 is a flowchart showing a method for the initial installation and subsequent use of pay-per-use software at a local machine in accordance with an aspect of the present invention.

Figure 3 is a flowchart showing a method according to an aspect of the present invention for managing a client-side (user) data processing apparatus for acquiring tokens.

Figure 4 is a flowchart showing a method for storing tokens according to an aspect of the present invention.

Figure 5 is a flowchart showing a continuation of the flowchart of Figure 4.

Figure 6 is a flowchart showing a method for consuming tokens at a data processing apparatus according to an aspect of the present invention.

Figure 7 is a flowchart showing a continuation of the flowchart of Figure 6.

Figure 8 is a flowchart showing a continuation of the flowchart of Figure 7.

Figure 9 is a flowchart showing a method according to an aspect of the present invention for managing a server-side (token provider) data processing apparatus for generating and providing tokens.

Figure 10 is a flowchart showing a continuation of the flowchart of Figure 9.

Detailed Description

Figure 1 shows a networked system 100 comprising a token provider server 102 connected to a plurality of workstations 106a-106c via a network 104. The networked system 100 is used to managed the distribution of tokens to the workstations that allow access to resources that are preferably contained within the workstations 106a-106c themselves. Workstation 106a is a portable computer used by a field service engineer that contains application software. The application software is configured to consume a token from the local hard disk drive when the engineer has finished using the application software and update the token record in the token record file. In this way, the application software can be used on a pay-per-use basis with tokens being consumed off-line without needing to be reconciled.

Tokens are downloaded to the workstations 106a-106c from the token provider server 102. Tokens are data objects each of which represents a specific monetary value and each of which is unique. Tokens are produced, or "minted", using algorithms that incorporate checking information with the token so as to reduce the chance of tokens being forged. The token provider server 102 maintains a database record of all tokens distributed to the workstations 106a-106c, their status and details of the customers to whom the tokens are distributed. The token provider server 102 also manages payment for the tokens by controlling credit and debit payments according to the status of a particular customer. Preferred customers are given credit accounts and can elect to distribute tokens amongst their engineers as they wish. Other customers may be required to make payment for tokens up-front or on a pay-as-you-go basis. Such customer requirements are also recorded by the token provider server 102 which then manages token distribution accordingly.

Figure 2 is a flowchart showing a method for the initial installation and subsequent use of pay-per-use application software stored at workstation 106a. Before the user can begin using the application software, it needs to be installed on the hard disk drive of the workstation 106a. At step 202 the application software is installed by the user using conventional methods such as by using removable program carrying installation media or by downloading the application software from the token provider server 102 via the network 104. Following initial installation, the application software

can be upgraded whenever the workstation 106a is in communication with the token provider server 102, should the token provider server 102 determine that such an upgrade is necessary.

After the application software has been installed, the user may attempt to access a function of the software that requires payment in order that the function be operable (step 204). Payment is made by consuming tokens purchased from the token provider. When the engineer attempts to access the restricted functions the application software, at step 206, checks the hard disk to see whether there are any tokens stored thereon that can be used to pay for using the function.

To look for the tokens, the application software checks the hard disk drive for a token record file. The token record file is used as a container to store tokens, associated information and user information securely on the hard disk drive of the workstation 106a, and is stored in an encrypted form to help prevent any user tampering. The encryption (and decryption) scheme uses a symmetric key encryption algorithm taking, for example, the hard disk drive's serial number as its key, so as to help ensure that the encrypted token record file is localised in use to the particular workstation 106a for which the tokens contained in the token record file were sold.

When no unspent tokens are available in a user's record (at step 208), the operation for which tokens are charged will fail to function. To remedy this, the user would have to collect more tokens from the token provider's server (at step 212). If tokens are available, and a chargeable operation is requested, then a token is consumed 210 (see Figures 6 to 8 and the following description). Where the process of consuming a local token 210 is successful, the function selected by the user for which payment is required is performed (at step 214). By allowing the consumption of tokens off-line, there is no need to provide for on-line token reconciliation with all its inherent disadvantages. For example, by storing the tokens locally on a user's hard disk drive, they may be rapidly accessed and consumed without awaiting on-line approval for their use.

Figure 3 is a flowchart depicting the method 300 operating client-side (user-side) on the workstation 106a by which tokens are acquired from the token provider server 102. In this embodiment the bulk of the method is invoked using a Java based plug-in, or applet, that runs in the user's web-browser, although here we note that this

part of the method may equally well be invoked from within the application software itself. Use of pre-existing web-browser software is preferred in this case as it avoids the need to code communications functionality and protocols into the application software.

At step 302 the application software launches the user's web-browser by calling the web-browser executable with a pointer to the Java applet. The web-browser then launches and when the applet starts it invokes the method illustrated in steps 304 through 314. The web-browser attempts at step 304 to connect to the token provider's web-site, via the internet, which in this case is hosted by the token provider server 102. The user is requested to provide identifying information and a corroborating password. Once a connection is established, a request is made for tokens to be supplied from the token provider server 102 to the workstation 106a (step 306). The request is then dealt with by the token provider server 102 which can release tokens, if available, to the workstation 106a. The token provider server 102 also checks the user identity and password.

If tokens are not available, or the token request is otherwise unsuccessful, a message is provided to the web-browser from the token provider server 102 indicating reasons for the failure to provide tokens and information on what steps the user should take next (step 310). If the user identification is accepted and the token request is successful, tokens and other information are transmitted to the workstation 106a, over a secure SSL/TLS connection established for the session. At step 312 the applet stores the tokens in an encrypted file on the hard disk drive of the workstation 106a and updates additional control information associated with the token record file to provide further token security (see Figures 4 and 5 and the corresponding description below). Information read from an existing token record file on the hard disk during the update process and the workstation 106a is transmitted at step 314 back to the token provider server 102 for analysis and storage. This information includes a count of the number of used and unused tokens, the hard disk serial number as well as the system time at the workstation 106a.

Figure 4 is a flowchart showing a method for storing tokens 312 on workstation 106a. Figure 5 is a flowchart showing a continuation of the flowchart of Figure 4. At step 402 encrypted tokens and time information are received at the workstation 106a.

The tokens, time information and other information may be transferred from the token provider server and/or the user's data processing apparatus over the secure SSL/TLS connection established for the session. Transfer of data in this fashion uses encryption by virtue of the underlying SSL/TLS protocol, and hence provides token security even if intervening networks are insecure.

Before any tokens are stored on the workstation 106a, the applet performs some housekeeping exercises on the hard disk. Firstly, a check of the hard disk is made at step 404 to determine if there is already a token record file in which the downloaded tokens and any additional information can be stored. At this point, any security verification files associated with the token record file and stored in one of a predetermined set of directories are also noted. If no such security verification file is found stored on the hard disk drive, an error is generated at step 406 that prevents the procedure for storing tokens from continuing. A message may be presented to a user at this point explaining what to do next.

At step 408 a check is performed to test whether the token record file is encrypted. If it is encrypted, the token record file information is decrypted using the hard disk drive serial number as the key. A check is then performed at step 410 to test whether the user is identified in the token record file. If the user is not identified by the token record file, an error is generated (at step 412) and the user is presented with a message explaining that no further tokens will be downloaded. If the user is positively identified, all previous security verification files on the hard disk drive are identified and deleted (step 414).

The tokens to be stored and their respective associated information are then appended to the decrypted pre-existing tokens and token information, at step 416, to form a new data object. The new data object then forms the input to a secure hashing algorithm (in this case SHA-1 is used at step 418) that calculates a 160 bit message digest corresponding to the new data object.

If the original token record file was encrypted, the new data object, corresponding to a new token record file, is encrypted using the hard disk drive serial number as a symmetric key. The token record file, either encrypted or unencrypted, is then stored in a first data storage area on the hard disk drive possibly using file path encoding (step 420).

In order to provide file path encoding, four bits such as for example bit 7 to bit 4 of the 160 bit message digest are used to determine in which directory path a file to which file path encoding is to be applied should be stored in so as to encode the four bits of data. To do this, a set of look-up tables is used. Bits 5 and 4 are used to produce a decimal primary index number from their binary values: i.e. 00 = 0, 01 = 1, 10 = 2 and 11 = 3. The primary index is used to determine a first partial path of the directory path, thus:

Primary Table

PathA = index 0
PathB = index 1
PathC = index 2
PathD = index 3

Having determined a first partial path, bits 7 and 6 are then used to produce a decimal secondary index number: i.e. 00 = 0, 01 = 1, 10 = 2 and 11 = 3. Each secondary index is associated with a secondary table. One such table, which is selected for the example where bits 5 and 4 of the message digest are binary 11, is shown as follows:

Secondary Table for index = 3

PathD_A = index 0
PathD_B = index 1
PathD_C = index 2
PathD_D = index 3

The secondary index, determined from the primary index, is then used to select a further partial path from the secondary table according to the value of bits 7 and 6. For example, if bits 7 and 6 are set to be binary 10, the secondary index equals two and so the further partial path selected would be PathD_C.

The full directory path, encoding the 4-bits of binary information, in which the file is stored is constructed as a concatenation of the first and the further partial paths as indexed by bits 7 to 4 (when read from MSB to LSB) of the message digest. For

example, if bits 7 to 4 are set as "1011", the file will be stored in directory \PathD\PathD_C.

All combinations of the paths need to be present in order that the file can be stored there. If any path does not exist, it must first be created. The paths selected are those that are ordinarily present on the hard disk drive of the workstation 106a. The primary table entries are:

c:\	- the windows root directory
c:\Program Files	- the program files directory
c:\windows	- the windows system path, could be "winNT"
c:\ElanPCCard	- Elan eMCE directory

For the windows root directory the secondary table entries are:

<none>	
\ElanPCCard	
\windows	- or "winNT"
\Program Files	

For the program files directory the secondary table entries are:

\Accessories	
\Common Files\Microsoft Shared\Dao	
\System\ole db	- or \Common Files\System\ole db
\Services	- or \Common Files\Services

For the windows system path directory the secondary table entries are:

\system	- or \system32
\system\drivers	- or \system32\drivers
\java	
\java\classes	

For the Elan eMCE (ElanPCCard) directory the secondary table entries are:

\eMCE
\eMCE\CardData
\eMCE\html
\eMCE\document

Having determined the directory in which to store the file using the file path encoding method, the file is then stored.

The file path encoding method as previously described is used to select the location in which a security verification file is stored (step 422). The content of the security verification file consists of a short random string of data stored using a predetermined filename. The path to the security verification file is selected as described previously, and different bits of the message digest can be used to select the file path if both the token record file and the security verification file use file path encodings. For example, bits 11 to 8 of the massage digest may be used, although any combination may be selected. It is even possible to encode using random bits of the message digest, the pattern of which is encrypted as part of the token record file, to provide for further security enhancement.

By way of additional security, a further 4-bits of data corresponding to, for example, bits 3 to 0 (MSB to LSB) of the message digest are steganographically hidden in a second data storage area of the hard disk drive. These 4-bits are encoded by modifying the time stamp data of the stored security verification file that is stored in a second data storage area by the file operating system. The process by which this is achieved is shown by steps 424 to 428.

Firstly, at step 424, the system time of the workstation 106a is read into a first variable following a call to the operating system. The number of seconds is then set to zero. The time stamp of both the last written and last accessed fields are then set to the modified system time value indicated by the variable (step 426). A data value corresponding to the 4-bit number taken from the message digest that is to be encoded is then subtracted as a number of seconds from the variable value. The variable value then indicates a reduced time that is saved as the new creation time of the security verification file (step 428). In this way, data is hidden on the disk in the data area reserved for recording file attributes.

At the end of the process of Figure 5, a security verification file is to be found stored on the hard disk drive of the workstation 106a along with other hidden control information that is used to verify the integrity of tokens and other data stored in the token record file.

Figure 6 is a flowchart showing a method for consuming tokens 210 at a workstation 106. Figures 7 and 8 are flowcharts showing a continuation of the

Nintendo Exhibit 1003
Part 1 of 2
Page 00478

flowchart that starts at Figure 6. This process is carried out by the application software that is stored at the workstations.

The process of consuming a token 210 begins, at step 602, with the application software searching the predetermined set of file location paths (see above) in which security verification files may be stored. A search is made to determine whether or not more than one security verification file exists (step 604). If more than one security verification file exists, then all but the most recent is deleted (step 606). A process of recovering the 8-bits of the message digest encoded by the security verification file then begins (steps 608 to 612). This works substantially by reversing each of the two processes used to encode the two sets of 4-bits in the first place. Optionally, an additional verification check is also made if the token record file also encodes part of the message digest.

The file location of the security verification file is determined during the search for the security verification file and accounting for any subsequent deletions. The bit pattern corresponding to four bits of the message digest used to determine the security verification file location are found by comparing the storage path to a set of tables and looking up the corresponding bit values (steps 608 and 610). Next, in step 612, the information corresponding to the four bits of the message digest used to determine the security verification file location are found from the file attribute information by subtracting the security verification file creation time from the security verification file written time.

The token record file is then decrypted in step 614 using the hard disk drive serial number as a symmetric key. The decrypted token record file data is then used as input to the same secure hashing algorithm that is used when the tokens are being stored to produce a message digest (step 616). Thereafter, the recovered steganographic bit pattern is compared to the respective bits of message digest (step 618). Any mismatch between these sets of data causes the consumption process to fail, during which process (step 622) a message is issued to the user and a record of failure is written to the hard disk drive.

Where the token record file has been validated, the application software searches the decrypted token record file for a token that has associated information indicating that it is valid (step 630). The token is then either marked as having been

used, or deleted to free up space in the token record file for new tokens that will be loaded at a later time. Having consumed a token, the token record file is re-encrypted and new control information calculated and used to store the encrypted token record file (steps 634 to 640), in much the same manner as is used to store new tokens as described above. Having consumed a token the application software then grants the user access to the protected resources.

Figure 9 is a flowchart showing a method 900 that is used at the token provider server 102 for generating and providing tokens. Figure 10 is a flowchart showing a continuation of the flowchart of Figure 9. The method is implemented as a software module or object running in conjunction with, or as part of, a stand-alone executable program to deal with individual requests for tokens.

The token provider server 102 is connected to a firewall web-server (not shown) that continuously monitors a communications link for external requests for information, tokens etc. The firewall server is operable to forward requests for service from external users to the token provider server 102 and to provide data from the token provider server 102 to the external users. Requests for tokens are passed from the firewall web-server to the token provider server 102. Additionally, the function of the firewall web-server is to provide standard information over an internet link to requesting parties, and to secure the token provider server 102 from external interference.

At step 902, the token provider server 102 receives a request for provision of tokens indirectly from an external user. The token provider server 102 then sends a request to the external user for his user identification (uid), password and the user's hard disk drive serial number (step 904). If a user identification and password are received in response to this request, a check is made in a database of user id's and passwords to see whether there is an entry for the provided uid and if so whether it corresponds to the password provided (steps 906 and 910). If there is no match in the database for the uid, or if the password does not match the uid, the token provider server 102 sends a message to the external user to say that the request to provide tokens has failed, and provides the reasons for the failure (step 908).

When an existing user is positively identified, a check is made at step 912 to see whether there are any tokens available to the user. Tokens may be made available

on credit for certain users (such as corporate users) or may have been paid for in advance via an online connection, over the telephone by credit/debit card, by post with a cheque etc. Advance payment for tokens is preferably performed separately from their provision to the user. The tokens, which are themselves sequentially chosen numbers, are then held in an SQL token database to which the token provider server 102 has access, and distributed to the users as necessary. If there are no tokens available to the user, the request for tokens is rejected at step 914. A rejection at this stage is accompanied by a message informing the user that tokens are unavailable, the reasons for this and what the user might do to remedy the situation.

Where tokens are available to the user, the user is informed at step 916 of the number of tokens at their disposal and prompted to request the number that are required to be downloaded to the user's machine. The user's request is sent to the token provider server 102 which then identifies the requested number of tokens in the SQL database to be sent to the user (step 918). At step 920 a secure session based upon SSL/TLS is setup between the token provider server 102 and the user's data processing apparatus 106. Tokens and other information, such as the time interval after which the tokens expire, is communicated to the user's data processing apparatus 106 by way of the secure session. Thereafter, the tokens and other information are processed at the user's data processing apparatus 106 according to the method 312 described above and illustrated in Figure 4 below.

Once the tokens have successfully been sent to the user, the tokens are marked in the SQL database as having been assigned to the user, and control information regarding the tokens is updated (step 922). As an additional check, the token provider server 102 sends a request to the user identified using an internal database record to request confirmation that the sent tokens have been received and stored without error. Any errors can be dealt with according to their nature, and the details of the error handling procedures are not deemed to require further explanation here. In addition to providing the token provider server 102 with a confirmation of a successful token transfer, a request for information regarding the status of the token record file held at the user's machine is requested (step 924). This status information could include the number of failed attempts there have been to consume tokens, the nature of any failures (time-expiry or possible fraudulent use) and an indication of the local time set

on the system clock of the user's machine. At step 926, the status information is uploaded to the token provider server 102 over the secure SSL/TLS session. This information is then stored at step 928 in the token database where it may subsequently be analysed to check for any suspicious user activity. At step 928 the user information is also updated, in particular a record of the number of tokens available to the user is decreased by the number of tokens that have just been successfully provided to the user's data processing apparatus 106.

Alternative embodiments of the invention generate keys for encrypting and decrypting token record files by combining a hard drive serial number with a random number to create a unique installation number. The unique installation number is stored in the token record file on the user's machine and on the token provider server during the signup process. The unique installation number is also used to identify the user in future communications.

Although the invention has been described in relation to the preceding example embodiments, it will be readily understood by those of ordinary skill in the art that many different embodiments employing the inventive concepts of the invention are possible. For example, although security verification files have been described in conjunction with the encoding of the eight least significant bits of a message digest, it is understood that any number of bits may be encoded using the techniques described. Furthermore, the bits selected for encoding may be selected, either individually or in any combination, from any bit position of a message digest and/or other such control information. Moreover, those skilled in the art will understand that the token record files themselves could also be used to encode control information and that any number of security verification files may be used to increase the number of bits of information hidden. It is the applicant's intention that all such variants fall within the scope of the invention.

The scope of the present disclosure includes any novel feature or combination of features disclosed therein either explicitly or implicitly or any generalisation thereof irrespective of whether or not it relates to the claimed invention or mitigates any or all of the problems addressed by the present invention. The applicant hereby gives notice that new claims may be formulated to such features during the prosecution of this application or of any such further application derived therefrom. In particular, with

Nintendo Exhibit 1003
Part 1 of 2
Page 00482

reference to the appended claims, features from dependent claims may be combined with those of the independent claims and features from respective independent claims may be combined in any appropriate manner and not merely in the specific combinations enumerated in the claims.

CLAIMS

1. A method for consuming non-reconciled tokens, said method comprising:

reading a stored token from a first storage area;

calculating control information corresponding to said stored token;

reading predetermined control information corresponding to said stored token from a second storage area, wherein said first storage area is separate from said second storage area;

comparing said control information to said predetermined control information; and

consuming said stored token conditional on said control information matching said predetermined control information.

2. The method of Claim 1, wherein said stored token is stored in a token record file.

3. The method of Claim 2, wherein said token record file further comprises information indicating an expiry time of said stored token.

4. The method of any preceding claim, wherein consumption of said stored token is further conditional upon a time interval between a last recorded update time and a current time not exceeding a predetermined value.

5. The method of any one of Claims 2 to 4, wherein said token record file further comprises user information corresponding to said stored token.

6. The method of any one of Claims 2 to 5, wherein said token record file further comprises information indicating whether said stored token is valid.

7. The method of any one of Claims 2 to 6, wherein at least one further token is stored in said token record file.

8. The method of Claim 7, wherein said token record file further comprises information indicating an expiry time of each of said at least one further token.

9. The method of Claim 7 or Claim 8, wherein said token record file further comprises user information corresponding to each of said at least one further token.

10. The method of any one of Claims 7 to 9, wherein said token record file further comprises information indicating whether each of said at least one further token is valid or not.

11. The method of any one of Claims 2 to 10, wherein said token record file is stored in an encrypted form in said first storage area.

12. The method of any one of Claims 2 to 11, wherein said step of calculating control information corresponding to said stored token comprises calculating a message digest from said token record file.

13. The method of any one of Claims 2 to 12, wherein said step of consuming said stored token comprises:

modifying said token record file by marking said stored token as having been used;

storing said modified token record file in place of said token record file in said first storage area;

calculating new predetermined control information from said modified token record file; and

storing said new predetermined control information in place of said control information in said second storage area.

14. The method of any preceding claim, comprising storing a security verification file in said second storage area.

15. The method of Claim 14, further comprising:

checking said second storage area for the presence of a plurality of security verification files; and

deleting all security verification files except the most recent security verification file.

16. The method of any preceding claim, wherein said first and second storage areas are located in a single data storage device.

17. The method of any preceding claim, wherein data stored in said second storage area is hidden using a steganographic hiding technique.

18. The method of any preceding claim, further comprising the step of enabling access to restricted access resources conditional on consumption of said stored token.

19. The method of any preceding claim, further comprising the step of enabling access to pay-per-access resources conditional on consumption of said stored token.

20. A method for storing consumable non-reconciled tokens, said method comprising:

receiving a token from a token provider;

storing said token in a first storage area;

obtaining predetermined control information corresponding to said token; and

storing said predetermined control information in a second storage area, wherein said first storage area is separate from said second storage area.

21. The method of Claim 20, wherein the step of storing said token in a first storage area comprises storing said token in a token record file.

22. The method of Claim 20 or Claim 21, comprising storing a security verification file in said second storage area.

23. The method of any one of Claims 20 to 22, further comprising storing information indicating a time of last access to said token provider.

24. The method of any one of Claims 21 to 23, further comprising storing user information corresponding to said token in said token record file.

25. The method of any one of Claims 21 to 24, further comprising storing information indicating whether said stored token is valid in said token record file.

26. The method of any one of Claims 21 to 25, wherein at least one further token is stored in said token record file.

27. The method of any one of Claims 21 to 26, wherein said token record file is stored in an encrypted form in said first storage area.

28. The method of any one of Claims 21 to 27, wherein said step of obtaining predetermined control information corresponding to said token comprises calculating said predetermined control information from said token record file.

29. The method of Claim 28, wherein said step of calculating said predetermined control information from said token record file comprises calculating a message digest from said token record file.

30. The method of any one of Claims 20 to 27, wherein said step of obtaining predetermined control information corresponding to said token comprises downloading said predetermined control information from said token provider.

31. The method of any one of Claims 20 to 30, wherein said token provider is a server.

32. The method of any one of Claims 20 to 31, further comprising:

checking said first storage area for the presence of a token record file and/or a security verification file(s); and

informing a user conditional on the token record file and/or security verification file(s), being absent that the user needs to register online before proceeding.

33. The method of any one of Claims 21 to 32, wherein said step of storing said token further comprises:

modifying said token record file to incorporate said token; and

storing said modified token record file in place of said token record file in said first storage area.

34. The method of any one of Claims 20 to 33, wherein said first and second storage areas are located in a single data storage device.

35. The method of any one of Claims 20 to 34, wherein data stored in said second storage area is hidden using a steganographic hiding technique.

36. A method for supplying consumable non-reconciled tokens, said method comprising:

generating a unique token;

storing a copy of said unique token in at least one data storage device; and

providing said unique token to a data processing apparatus for storage in a first storage area, wherein said data processing apparatus is operable to store predetermined control information corresponding to said unique token in a second storage area separate from said first storage area.

37. The method of Claim 36, wherein said unique token is stored in a token record file in said first storage area.

38. The method of Claim 36 or Claim 37, further comprising providing information indicating an expiry time of said unique token to said data processing apparatus.

39. The method of Claim 38, further comprising storing a copy of said information indicating an expiry time of said unique token in said at least one data storage device.

40. The method of Claim 38 or Claim 39, wherein said information indicating an expiry time of said unique token is a time interval.

41. The method of any one of Claims 36 to 40, wherein said unique token is generated using user information.

42. The method of any one of Claims 36 to 41, further comprising providing information indicating that said unique token is valid to said data processing apparatus.

43. The method of any one of Claims 36 to 42, further comprising reading a number indicating how many consumed tokens reside on said data processing apparatus from said data processing apparatus.

44. The method of Claim 43, further comprising blocking the provision of further tokens to said data processing apparatus conditional on said number of consumed tokens residing on said data processing apparatus not exceeding a first predetermined value.

45. The method of any one of Claims 36 to 44, further comprising reading a number indicating how many unused tokens reside on said data processing apparatus from said data processing apparatus.

46. The method of Claim 45, further comprising blocking the provision of further tokens to said data processing apparatus conditional on said number of unused tokens residing on said data processing apparatus equalling or exceeding a second predetermined value.

47. The method of any one of Claims 36 to 46, wherein a security verification file is stored in said second data storage area.

48. The method of any one of Claims 36 to 47, comprising:

reading said predetermined control information from said data processing apparatus;

reading said unique token from said data processing apparatus;

calculating control information from said copy of said unique token; and

comparing said predetermined control information to said calculated control information to determine whether there is a match, wherein an inexact match indicates fraudulent activity.

49. The method of Claim 48, further comprising blocking the provision of further tokens to said data processing apparatus conditional on said predetermined control information not being an exact match to said calculated control information.

50. The method of Claim 48 or Claim 49, when dependant upon Claim 37, wherein said step of calculating control information corresponding to said unique token comprises calculating a message digest from said token record file.

51. The method of any one of Claims 37 to 50, wherein said token record file is stored in an encrypted form in said first storage area.

52. The method of any one of Claims 36 to 51, wherein said first and second storage areas are located in a single data storage device.

53. The method of any one of Claims 36 to 52, wherein data stored in said second storage area is hidden using a steganographic hiding technique.

54. The method of any one of Claims 36 to 53, wherein said step of providing said unique token to said data processing apparatus further comprises taking prepayment in exchange for said unique token.

55. The method of any one of Claims 36 to 54, wherein said step of providing said unique token to said data processing apparatus further comprises charging a sum to a pre-existing customer credit account in exchange for said unique token.

56. The method of any one of Claims 36 to 55, further comprising downloading a software update to said data processing apparatus.

57. A computer program operable to configure a data processing apparatus to implement a method according to any one of Claims 1 to 56.

58. A computer carrier medium carrying a computer program according to Claim 57.

59. A data processing apparatus for providing access to resources in exchange for consumption of a consumable non-reconciled token, said data processing apparatus comprising:

a controller operable to access at least one data storage device, wherein said at least one data storage device is configured to provide at least a first and a separate second storage area, wherein said first storage area contains data encoding a

stored token and said second storage area contains data encoding predetermined control information corresponding to said stored token; and

a processor configured to:

a) read said stored token from said first storage area;

b) calculate control information corresponding to said stored token;

c) read predetermined control information corresponding to said stored token from said second storage area;

d) compare said control information to said predetermined control information; and

e) permit access to resources and consume said stored token conditional on said control information matching said predetermined control information.

60. The data processing apparatus of Claim 59, wherein said stored token is stored in a token record file.

61. The data processing apparatus of Claim 60, wherein said token record file further comprises information indicating an expiry time of said stored token.

62. The data processing apparatus of any one of Claims 59 to 61, wherein consumption of said stored token is further conditional upon a time interval between a last recorded update time and a current time not exceeding a predetermined value.

63. The data processing apparatus of any one of Claims 60 to 62, wherein said token record file further comprises user information corresponding to said stored token.

64. The data processing apparatus of Claims 60 to 63, wherein said token record file further comprises information indicating whether said stored token is valid.

65. The data processing apparatus of Claims 60 to 64, wherein at least one further token is stored in said token record file.

66. The data processing apparatus of Claim 65, wherein said token record file further comprises information indicating an expiry time of each of said at least one further token.

67. The data processing apparatus of Claim 65 or Claim 66, wherein said token record file further comprises user information corresponding to each of said at least one further token.

68. The data processing apparatus of any one of Claims 65 to 67, wherein said token record file further comprises information indicating whether each of said at least one further token is valid or not.

69. The data processing apparatus of any one of Claims 60 to 68, wherein said token record file is stored in an encrypted form in said first storage area and said step of reading said stored token from said first storage area comprises decrypting said encrypted token record file and extracting said stored token.

70. The data processing apparatus of any one of Claims 60 to 69, wherein said processor is configured to calculate control information corresponding to said stored token by calculating a message digest from said token record file.

71. The data processing apparatus of any one of Claims 60 to 70, wherein said processor is configured to consume said stored token by:

modifying said token record file by marking said stored token as having been used;

storing said modified token record file in place of said token record file in said first storage area;

calculating new predetermined control information from said modified token record file; and

storing said new predetermined control information in place of said control information in said second storage area.

72. The data processing apparatus of any one of Claims 59 to 71, wherein said processor is configured to store a security verification file in said second storage area.

73. The data processing apparatus of Claim 72, wherein said processor is further configured to:

check said second storage area for the presence of a plurality of security verification files; and

delete all security verification files except the most recent security verification file.

74. The data processing apparatus of any one of Claims 59 to 73, wherein said first and second storage areas are located in a single data storage device.

75. The data processing apparatus of any one of Claims 59 to 74, wherein data stored in said second storage area is hidden using a steganographic hiding technique.

76. The data processing apparatus of any one of Claims 59 to 75, wherein said resources comprise a software application.

77. The data processing apparatus of Claim 76, wherein said processor is configured to consume said stored token when data is saved from said software application.

78. A data processing apparatus for generating and distributing consumable non-reconciled tokens, said data processing apparatus comprising:

a communications interface;

at least one data storage device; and

a processor configured to:

a) generate a unique token;

b) store a copy of said unique token in said at least one data storage device; and

c) provide said unique token via said communications interface to a further data processing apparatus for storage in a first storage area, wherein said data processing apparatus is operable to store predetermined control information corresponding to said unique token in a second storage area separate from said first storage area.

79. The data processing apparatus of Claim 78, wherein said further data processing apparatus is operable to store said unique token in a token record file in said first storage area.

80. The data processing apparatus of Claim 78 or Claim 79, wherein said processor is further configured to provide time information to said further data processing apparatus.

81. The data processing apparatus of Claim 80, wherein said time information is a time interval after which tokens are unusable.

82. The data processing apparatus of Claim 80 or Claim 81, wherein said processor is further configured to store a copy of time information in said at least one data storage device.

83. The data processing apparatus of any one of Claims 78 to 82, wherein said processor is configured to generate said unique token using user information.

84. The data processing apparatus of any one of Claims 78 to 83, wherein said processor is configured to provide information to said further data processing apparatus indicating that said unique token is valid.

85. The data processing apparatus of any one of Claims 78 to 84, wherein said processor is configured to read from said further data processing apparatus a number indicating how many consumed tokens reside on said further data processing apparatus.

86. The data processing apparatus of Claim 85, wherein said processor is configured to block the provision of further tokens to said further data processing apparatus conditional on said number of consumed tokens not exceeding a first predetermined value.

87. The data processing apparatus of any one of Claims 78 to 86, wherein said processor is configured to read from said further data processing apparatus a number indicating how many unused tokens reside on said further data processing apparatus.

88. The data processing apparatus of Claim 87, wherein said processor is configured to block the provision of further tokens to said further data processing apparatus conditional on said number of unused tokens equalling or exceeding a second predetermined value.

89. The data processing apparatus of any one of Claims 78 to 88, wherein a security verification file is stored in said second data storage area.

90. The data processing apparatus of any one of Claims 78 to 89, wherein said processor is further configured to:

read said predetermined control information from said further data processing apparatus;

read said unique token from said further data processing apparatus;

calculate control information from said copy of said unique token; and

compare said predetermined control information to said calculated control information to determine whether there is a match, an inexact match being indicative of possible fraudulent activity.

91. The data processing apparatus of Claim 90, wherein said processor is configured to block the provision of further tokens to said further data processing apparatus conditional on said predetermined control information not being an exact match to said calculated control information.

92. The data processing apparatus of Claim 90 or Claim 91, when dependant upon Claim 79, wherein said processor is configured to calculate said control information by calculating a message digest from said token record file.

93. The data processing apparatus of any one of Claims 78 to 92, wherein said processor is operable to encrypt said unique token before providing an encrypted version of said unique token via said communications interface.

94. The data processing apparatus of any one of Claims 78 to 93, wherein said first and second storage areas of said further data processing apparatus are located in a single data storage device.

95. The data processing apparatus of any one of Claims 78 to 94, wherein data stored in said second storage area of said further data processing apparatus is hidden using a steganographic hiding technique.

96. The data processing apparatus of any one of Claims 78 to 95, wherein said processor is configured to provide said unique token to said further data processing apparatus in exchange for a prepayment.

97. The data processing apparatus of any one of Claims 78 to 96, wherein said processor is configured to provide said unique token to said further data processing apparatus following addition of a charge to a pre-existing customer credit account.

98. The data processing apparatus of any one of Claims 78 to 97, wherein said processor is configured to supply a software update to said further data processing apparatus.

99. A method for hiding data, comprising:

generating a digital fingerprint from a data file stored in a first storage area; and

hiding said digital fingerprint by storing at least part of said digital fingerprint in a second storage area, wherein said first storage area is separate from said second storage area.

100. The method of Claim 99, wherein said second storage area is not directly user-accessible.

101. The method of Claim 99 or Claim 100, wherein said digital fingerprint is a message digest generated from at least said data file.

102. The method of any one of Claims 99 to 101, wherein said at least part of said digital fingerprint is hidden using a steganographic technique.

103. The method of Claim 102, wherein said steganographic technique comprises encoding at least one bit of said digital fingerprint by storing a security verification file at one location selected from a plurality of predetermined file locations.

104. The method of Claim 103, wherein said steganographic technique comprises encoding at least one further bit of said digital fingerprint by modifying a file time stamp of said security verification file.

105. The method of Claim 102, wherein said steganographic technique comprises encoding at least one bit of said digital fingerprint by modifying a file time stamp of a security verification file.

106. A system for generating and distributing tokens substantially as hereinbefore described with reference to Figure 1 of the accompanying drawings.

107. A method for the initial installation and subsequent use of pay-per-use software at a data processing apparatus substantially as hereinbefore described with reference to Figure 2 of the accompanying drawings.

108. A method for acquiring tokens substantially as hereinbefore described with reference to Figure 3 of the accompanying drawings.

109. A method for storing consumable non-reconciled tokens substantially as hereinbefore described with reference to Figures 4 and 5 of the accompanying drawings.

110. A method for consuming non-reconciled tokens substantially as hereinbefore described with reference to Figures 6 to 8 of the accompanying drawings.

111. A method for generating and providing consumable non-reconciled tokens substantially as hereinbefore described with reference to Figures 9 and 10 of the accompanying drawings.

112. A computer program substantially as hereinbefore described with reference to the method of any one of Figures 2 to 10 of the accompanying drawings.

113. A data processing apparatus for providing access to resources in exchange for consumption of a consumable non-reconciled token substantially as hereinbefore described.

114. A data processing apparatus for generating and distributing consumable non-reconciled tokens substantially as hereinbefore described.

Amendments to the claims have been filed as follows

CLAIMS

1. A method for consuming non-reconciled tokens, said method comprising:

reading a stored token from a first storage area;

calculating control information corresponding to said stored token;

reading predetermined control information corresponding to said stored token from a second storage area, wherein said first storage area is separate from said second storage area;

comparing said control information to said predetermined control information; and

consuming said stored token conditional on said control information matching said predetermined control information.

2. The method of Claim 1, wherein said stored token is stored in a token record file.

3. The method of Claim 2, wherein said token record file further comprises information indicating an expiry time of said stored token.

4. The method of any preceding claim, wherein consumption of said stored token is further conditional upon a time interval between a last recorded update time and a current time not exceeding a predetermined value.

5. The method of any one of Claims 2 to 4, wherein said token record file further comprises user information corresponding to said stored token.

6. The method of any one of Claims 2 to 5, wherein said token record file further comprises information indicating whether said stored token is valid.

7. The method of any one of Claims 2 to 6, wherein at least one further token is stored in said token record file.

8. The method of Claim 7, wherein said token record file further comprises information indicating an expiry time of each of said at least one further token.

9. The method of Claim 7 or Claim 8, wherein said token record file further comprises user information corresponding to each of said at least one further token.

10. The method of any one of Claims 7 to 9, wherein said token record file further comprises information indicating whether each of said at least one further token is valid or not.

11. The method of any one of Claims 2 to 10, wherein said token record file is stored in an encrypted form in said first storage area.

12. The method of any one of Claims 2 to 11, wherein said step of calculating control information corresponding to said stored token comprises calculating a message digest from said token record file.

13. The method of any one of Claims 2 to 12, wherein said step of consuming said stored token comprises:

modifying said token record file by marking said stored token as having been used;

storing said modified token record file in place of said token record file in said first storage area;

calculating new predetermined control information from said modified token record file; and

storing said new predetermined control information in place of said control information in said second storage area.

14. The method of any preceding claim, comprising storing a security verification file in said second storage area.

15. The method of Claim 14, further comprising:

checking said second storage area for the presence of a plurality of security verification files; and

deleting all security verification files except the most recent security verification file.

16. The method of any preceding claim, wherein said first and second storage areas are located in a single data storage device.

17. The method of any preceding claim, wherein data stored in said second storage area is hidden using a steganographic hiding technique.

18. The method of any preceding claim, further comprising the step of enabling access to restricted access resources conditional on consumption of said stored token.

19. The method of any preceding claim, further comprising the step of enabling access to pay-per-access resources conditional on consumption of said stored token.

20. A method for storing consumable non-reconciled tokens, said method comprising:

receiving a token from a token provider;

storing said token in a first storage area;

obtaining predetermined control information corresponding to said token; and

storing said predetermined control information in a second storage area, wherein said first storage area is separate from said second storage area.

21. The method of Claim 20, wherein the step of storing said token in a first storage area comprises storing said token in a token record file.

22. The method of Claim 20 or Claim 21, comprising storing a security verification file in said second storage area.

23. The method of any one of Claims 20 to 22, further comprising storing information indicating a time of last access to said token provider.

24. The method of any one of Claims 21 to 23, further comprising storing user information corresponding to said token in said token record file.

25. The method of any one of Claims 21 to 24, further comprising storing information indicating whether said stored token is valid in said token record file.

26. The method of any one of Claims 21 to 25, wherein at least one further token is stored in said token record file.

27. The method of any one of Claims 21 to 26, wherein said token record file is stored in an encrypted form in said first storage area.

28. The method of any one of Claims 21 to 27, wherein said step of obtaining predetermined control information corresponding to said token comprises calculating said predetermined control information from said token record file.

29. The method of Claim 28, wherein said step of calculating said predetermined control information from said token record file comprises calculating a message digest from said token record file.

30. The method of any one of Claims 20 to 27, wherein said step of obtaining predetermined control information corresponding to said token comprises downloading said predetermined control information from said token provider.

31. The method of any one of Claims 20 to 30, wherein said token provider is a server.

32. The method of any one of Claims 20 to 31, further comprising:

checking said first storage area for the presence of a token record file and/or a security verification file(s); and

informing a user conditional on the token record file and/or security verification file(s), being absent that the user needs to register online before proceeding.

33. The method of any one of Claims 21 to 32, wherein said step of storing said token further comprises:

modifying said token record file to incorporate said token; and

storing said modified token record file in place of said token record file in said first storage area.

34. The method of any one of Claims 20 to 33, wherein said first and second storage areas are located in a single data storage device.

35. The method of any one of Claims 20 to 34, wherein data stored in said second storage area is hidden using a steganographic hiding technique.

36. A method for supplying consumable non-reconciled tokens, said method comprising:

generating a unique token;

storing a copy of said unique token in at least one data storage device;

providing said unique token to a data processing apparatus to store in a first storage area; and

operating said data processing apparatus to store predetermined control information corresponding to said unique token in a second storage area separate from said first storage area.

37. The method of Claim 36, wherein said unique token is stored in a token record file in said first storage area.

38. The method of Claim 36 or Claim 37, further comprising providing information indicating an expiry time of said unique token to said data processing apparatus.

39. The method of Claim 38, further comprising storing a copy of said information indicating an expiry time of said unique token in said at least one data storage device.

40. The method of Claim 38 or Claim 39, wherein said information indicating an expiry time of said unique token is a time interval.

41. The method of any one of Claims 36 to 40, wherein said unique token is generated using user information.

42. The method of any one of Claims 36 to 41, further comprising providing information indicating that said unique token is valid to said data processing apparatus.

43. The method of any one of Claims 36 to 42, further comprising reading a number indicating how many consumed tokens reside on said data processing apparatus from said data processing apparatus.

44. The method of Claim 43, further comprising blocking the provision of further tokens to said data processing apparatus conditional on said number of consumed tokens residing on said data processing apparatus not exceeding a first predetermined value.

45. The method of any one of Claims 36 to 44, further comprising reading a number indicating how many unused tokens reside on said data processing apparatus from said data processing apparatus.

46. The method of Claim 45, further comprising blocking the provision of further tokens to said data processing apparatus conditional on said number of unused tokens residing on said data processing apparatus equalling or exceeding a second predetermined value.

47. The method of any one of Claims 36 to 46, wherein a security verification file is stored in said second data storage area.

48. The method of any one of Claims 36 to 47, comprising:

reading said predetermined control information from said data processing apparatus;

reading said unique token from said data processing apparatus;

calculating control information from said copy of said unique token; and

comparing said predetermined control information to said calculated control information to determine whether there is a match, wherein an inexact match indicates fraudulent activity.

49. The method of Claim 48, further comprising blocking the provision of further tokens to said data processing apparatus conditional on said predetermined control information not being an exact match to said calculated control information.

50. The method of Claim 48 or Claim 49, when dependant upon Claim 37, wherein said step of calculating control information corresponding to said unique token comprises calculating a message digest from said token record file.

51. The method of any one of Claims 37 to 50, wherein said token record file is stored in an encrypted form in said first storage area.

52. The method of any one of Claims 36 to 51, wherein said first and second storage areas are located in a single data storage device.

53. The method of any one of Claims 36 to 52, wherein data stored in said second storage area is hidden using a steganographic hiding technique.

54. The method of any one of Claims 36 to 53, wherein said step of providing said unique token to said data processing apparatus further comprises taking prepayment in exchange for said unique token.

55. The method of any one of Claims 36 to 54, wherein said step of providing said unique token to said data processing apparatus further comprises charging a sum to a pre-existing customer credit account in exchange for said unique token.

56. The method of any one of Claims 36 to 55, further comprising downloading a software update to said data processing apparatus.

57. A computer program operable to configure a data processing apparatus to implement a method according to any one of Claims 1 to 56.

58. A computer carrier medium carrying a computer program according to Claim 57.

59. A data processing apparatus for providing access to resources in exchange for consumption of a consumable non-reconciled token, said data processing apparatus comprising:

a controller operable to access at least one data storage device, wherein said at least one data storage device is configured to provide at least a first and a separate second storage area, wherein said first storage area contains data encoding a

stored token and said second storage area contains data encoding predetermined control information corresponding to said stored token; and

a processor configured to:

a) read said stored token from said first storage area;

b) calculate control information corresponding to said stored token;

c) read predetermined control information corresponding to said stored token from said second storage area;

d) compare said control information to said predetermined control information; and

e) permit access to resources and consume said stored token conditional on said control information matching said predetermined control information.

60. The data processing apparatus of Claim 59, wherein said stored token is stored in a token record file.

61. The data processing apparatus of Claim 60, wherein said token record file further comprises information indicating an expiry time of said stored token.

62. The data processing apparatus of any one of Claims 59 to 61, wherein consumption of said stored token is further conditional upon a time interval between a last recorded update time and a current time not exceeding a predetermined value.

63. The data processing apparatus of any one of Claims 60 to 62, wherein said token record file further comprises user information corresponding to said stored token.

64. The data processing apparatus of Claims 60 to 63, wherein said token record file further comprises information indicating whether said stored token is valid.

65. The data processing apparatus of Claims 60 to 64, wherein at least one further token is stored in said token record file.

66. The data processing apparatus of Claim 65, wherein said token record file further comprises information indicating an expiry time of each of said at least one further token.

67. The data processing apparatus of Claim 65 or Claim 66, wherein said token record file further comprises user information corresponding to each of said at least one further token.

68. The data processing apparatus of any one of Claims 65 to 67, wherein said token record file further comprises information indicating whether each of said at least one further token is valid or not.

69. The data processing apparatus of any one of Claims 60 to 68, wherein said token record file is stored in an encrypted form in said first storage area and said step of reading said stored token from said first storage area comprises decrypting said encrypted token record file and extracting said stored token.

70. The data processing apparatus of any one of Claims 60 to 69, wherein said processor is configured to calculate control information corresponding to said stored token by calculating a message digest from said token record file.

71. The data processing apparatus of any one of Claims 60 to 70, wherein said processor is configured to consume said stored token by:

modifying said token record file by marking said stored token as having been used;

storing said modified token record file in place of said token record file in said first storage area;

calculating new predetermined control information from said modified token record file; and

storing said new predetermined control information in place of said control information in said second storage area.

72. The data processing apparatus of any one of Claims 59 to 71, wherein said processor is configured to store a security verification file in said second storage area.

73. The data processing apparatus of Claim 72, wherein said processor is further configured to:

check said second storage area for the presence of a plurality of security verification files; and

delete all security verification files except the most recent security verification file.

74. The data processing apparatus of any one of Claims 59 to 73, wherein said first and second storage areas are located in a single data storage device.

75. The data processing apparatus of any one of Claims 59 to 74, wherein data stored in said second storage area is hidden using a steganographic hiding technique.

76. The data processing apparatus of any one of Claims 59 to 75, wherein said resources comprise a software application.

77. The data processing apparatus of Claim 76, wherein said processor is configured to consume said stored token when data is saved from said software application.

78. A data processing apparatus for generating and distributing consumable non-reconciled tokens, said data processing apparatus comprising:

a communications interface;

at least one data storage device; and

a processor configured to:

a) generate a unique token;

b) store a copy of said unique token in said at least one data storage device; and

c) provide said unique token via said communications interface to a further data processing apparatus for storage in a first storage area, wherein said data processing apparatus is operable to store predetermined control information corresponding to said unique token in a second storage area of the further data processing apparatus separate from said first storage area.

79. The data processing apparatus of Claim 78, wherein said further data processing apparatus is operable to store said unique token in a token record file in said first storage area.

80. The data processing apparatus of Claim 78 or Claim 79, wherein said processor is further configured to provide time information to said further data processing apparatus.

81. The data processing apparatus of Claim 80, wherein said time information is a time interval after which tokens are unusable.

82. The data processing apparatus of Claim 80 or Claim 81, wherein said processor is further configured to store a copy of time information in said at least one data storage device.

83. The data processing apparatus of any one of Claims 78 to 82, wherein said processor is configured to generate said unique token using user information.

84. The data processing apparatus of any one of Claims 78 to 83, wherein said processor is configured to provide information to said further data processing apparatus indicating that said unique token is valid.

85. The data processing apparatus of any one of Claims 78 to 84, wherein said processor is configured to read from said further data processing apparatus a number indicating how many consumed tokens reside on said further data processing apparatus.

86. The data processing apparatus of Claim 85, wherein said processor is configured to block the provision of further tokens to said further data processing apparatus conditional on said number of consumed tokens not exceeding a first predetermined value.

87. The data processing apparatus of any one of Claims 78 to 86, wherein said processor is configured to read from said further data processing apparatus a number indicating how many unused tokens reside on said further data processing apparatus.

88. The data processing apparatus of Claim 87, wherein said processor is configured to block the provision of further tokens to said further data processing apparatus conditional on said number of unused tokens equalling or exceeding a second predetermined value.

89. The data processing apparatus of any one of Claims 78 to 88, wherein a security verification file is stored in said second data storage area.

90. The data processing apparatus of any one of Claims 78 to 89, wherein said processor is further configured to:

read said predetermined control information from said further data processing apparatus;

read said unique token from said further data processing apparatus;

calculate control information from said copy of said unique token; and

compare said predetermined control information to said calculated control information to determine whether there is a match, an inexact match being indicative of possible fraudulent activity.

91. The data processing apparatus of Claim 90, wherein said processor is configured to block the provision of further tokens to said further data processing apparatus conditional on said predetermined control information not being an exact match to said calculated control information.

92. The data processing apparatus of Claim 90 or Claim 91, when dependant upon Claim 79, wherein said processor is configured to calculate said control information by calculating a message digest from said token record file.

93. The data processing apparatus of any one of Claims 78 to 92, wherein said processor is operable to encrypt said unique token before providing an encrypted version of said unique token via said communications interface.

94. The data processing apparatus of any one of Claims 78 to 93, wherein said first and second storage areas of said further data processing apparatus are located in a single data storage device.

95. The data processing apparatus of any one of Claims 78 to 94, wherein data stored in said second storage area of said further data processing apparatus is hidden using a steganographic hiding technique.

96. The data processing apparatus of any one of Claims 78 to 95, wherein said processor is configured to provide said unique token to said further data processing apparatus in exchange for a prepayment.

97. The data processing apparatus of any one of Claims 78 to 96, wherein said processor is configured to provide said unique token to said further data processing apparatus following addition of a charge to a pre-existing customer credit account.

98. The data processing apparatus of any one of Claims 78 to 97, wherein said processor is configured to supply a software update to said further data processing apparatus.

99. A system for providing access to resources in exchange for a consumption of a token substantially as hereinbefore described with reference to Figure 1 of the accompanying drawings.

100. A method for the initial installation and subsequent use of pay-per-use software at a data processing apparatus substantially as hereinbefore described with reference to Figure 2 of the accompanying drawings.

101. A method for managing a client-side data processing apparatus for acquiring tokens substantially as hereinbefore described with reference to Figure 3 of the accompanying drawings.

102. A method for storing consumable non-reconciled tokens substantially as hereinbefore described with reference to Figures 4 and 5 of the accompanying drawings.

103. A method for consuming non-reconciled tokens substantially as hereinbefore described with reference to Figures 6 to 8 of the accompanying drawings.

104. A method for managing a server-side data processing apparatus for generating and providing tokens substantially as hereinbefore described with reference to Figures 9 and 10 of the accompanying drawings.

105. A computer program operable to implement the method of any one of Figures 2 to 10 of the accompanying drawings.

Nintendo Exhibit 1003
Part 1 of 2
Page 00514

106. A data processing apparatus for providing access to resources in exchange for consumption of a consumable non-reconciled token substantially as hereinbefore described.

107. A data processing apparatus for generating and distributing consumable non-reconciled tokens substantially as hereinbefore described.

Application No: GB 0119846.4 **Examiner:** D Midgley
Claims searched: 1-98 **Date of search:** 28 March 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): G4A AAP

Int Cl (Ed.7): G06F 1/00,12/14,17/60

Other: ONLINE:WPI,EPODOC,JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	WO 99/27475 A1 (BARKAN)	1,20,36,59 and 78
A	US 5930777 (BARBER)	"

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Nintendo Exhibit 1003
Part 1 of 2
Page 00516

INVESTOR IN PEOPLE

Application No:	GB 0119846.4	**Examiner:**	D Midgley
Claims searched:	99-105	**Date of search:**	15 August 2002

Patents Act 1977
Further Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): G4A AAP

Int Cl (Ed.7): G06F1/00,12/14,17/60

Other: ONLINE:WPI,EPODOC,JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP 1056010 A1	(HEWLETT PACKARD) Whole doc.	99-101
X	EP 1030237 A1	(HEWLETT PACKARD) See, for example, column 7, lines 15-21.	"
X	WO 00/48063 A1	(WILDER et al) See, for example, page 7, lines 25-28	"
X	WO 95/15522 A1	(SCHEELE et al) See, for example, page 4, lines 3-6	"
X	US 5944821	(COMPAQ) See, for example, column 4, lines 41-50	"
X	US 5619571	(EWERT et al) See column 6, lines 1-8	"
X	US 5421006	(COMPAQ) Whole doc.	"

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 384 610 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **90301253.2**

(51) Int. Cl.5: **G06F 1/00**

(22) Date of filing: **06.02.90**

(30) Priority: **24.02.89 US 315071**

(43) Date of publication of application:
29.08.90 Bulletin 90/35

(84) Designated Contracting States:
DE ES FR GB

(71) Applicant: **International Business Machines Corporation**
Old Orchard Road
Armonk, N.Y. 10504(US)

(72) Inventor: **Enescu, Michael Alexander**
870 East El Camino Real 529
Sunnyvale, CA 94087(US)
Inventor: **Lum, James**
34 Cape Hatteras Court
Redwood City, CA 94065(US)

(74) Representative: **Grant, Iain Murray**
IBM United Kingdom Limited Intellectual Property Department Hursley Park
Winchester Hampshire SO21 2JN(GB)

(54) Tamper resistant access authorising method.

(57) A tamper-resistant facility is disclosed for controlling the number of users given authorised access to licensed software in a host-based, multiple terminal system by use of an encrypted authorisation list depth parameter. The facility can be embedded in the host-licensed software and can decrypt the depth parameter only using a key derived from its own CPU ID and an offset.

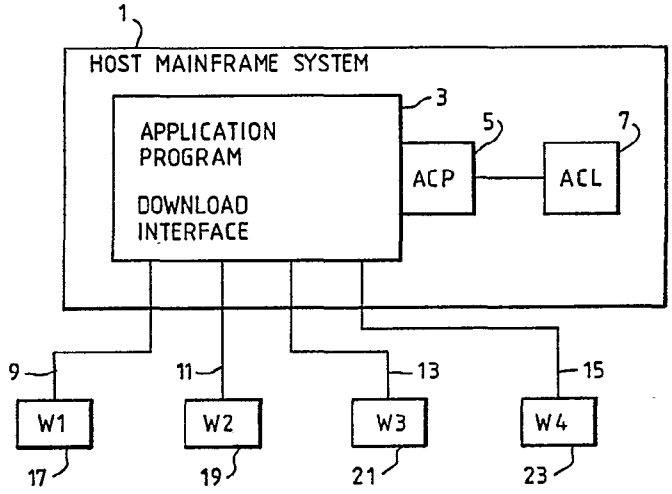


Fig. 1

EP 0 384 610 A2

Nintendo Exhibit 1003
Part 1 of 2
Page 00518

TAMPER RESISTANT ACCESS AUTHORISING METHOD

The present invention relates to computer system security and, more particularly, to a tamper resistant access authorising method for controlling the access of programs, processes, or users to resources defined by a computer system.

Reference should be made to Peterson and Silberschatz, "Operating System Concepts", copyright 1983 by Addison- Wesley Publishing Co., Chapter 11, relating to protection at pp. 387-419; and Dorothy Denning, "Cryptography and Data Security", copyright 1982 by Addison-Wesley Publishing Co., Chapter 4, relating to access controls at pp. 209-230.

These references describe mechanisms for controlling the access of programs, processes, or users to resources defined by a computer system. Both Peterson and Denning apparently favour an access matrix, either statically or dynamically implemented, to be the protection construct of choice in such systems.

The matrix construct uses rows to represent domains and columns to represent objects. Each entry in the matrix consists of a set of access rights. If a computer held a global table consisting of a set of ordered triples <user(i), object(j), rights set(k)>, then whenever an operation M was executed on an object O(j) by user U(i), a search would be made for the triple <U(i) ,O(j) ,R(k)> and the operation would be allowed to continue only upon a comparison match.

Both references further describe several constructs derived from an access matrix. These include access lists, capability lists, and lock and key mechanisms. It should be appreciated that an access list is list oriented, a capability list is ticket oriented, and a lock and key mechanism combines features of both.

An access list is no more than a set of ordered pairs <U(i), R(k)> sorted on each object O(j). A capability list is a transferrable set of ordered pairs <O(j), R(k)>. The capability is a ticket authorising any bearer (user in possession) R access rights to object O. Simple possession means that access is allowed.

With a lock and key mechanism, each object O(j) includes a unique bit pattern denominated a "lock", while only designated ones of the users are in possession of a unique bit pattern denominated a "key". Thus, a U(i) can obtain a key to O(j) only if he has access rights R(k) of a predetermined type.

Dunham et al., U.S. Patent 4,791,565, "Apparatus for Controlling the Use of Computer Software", issued December 13, 1988, illustrates the "access control list" construct. In this case, the "access rights" are used to police license restrictions. Dunham uses an EPROM-based microprocessor as a dedicated server. In this arrangement, software usage requests, emanating from terminals and destined for a host computer, are mediated before transmission. Each request is either passed on with or without comment, or rejected, all according to criteria recited in the user software license.

Pailen et al., U.S. Patent 4,652,990, "Protected Software Access Control Apparatus and Method", issued March 24, 1987, illustrates a "lock and key" approach to limiting unpermitted copying. In Pailen, an interactive encrypted message generation process among a requesting remote terminal and a pair of mediating processors is used to check that user, object, and rights match prior to granting access.

Wolfe, U.S. Patent 4,796,220, "Method of Controlling the Copying of Software", issued January 3, 1989, discloses another lock and key approach in which configuration information of authorised terminals is used as part of a permission code computation sent by a host to the requesting terminal. The computation is appended to each request and operates together with the configuration data as a key for recomputation of the code on subsequent access requests made by the terminal to the host.

From one aspect, the present invention provides a method for authorising access to application software resident in a CPU host from among N < M workstations or users communicatively attaching the CPU host, comprising the steps of:

(a) forming a list of authorised users and encrypting thereon a depth parameter N, the encryption using a function of the CPU identity and an offset as a key;

(b) responsive to each application software access request from among the workstations or users, accessing the list and decrypting the depth parameter N with the key; and

(c) scanning the list within the depth N and returning an access authorisation to the requester only upon an identity match.

Such a method in considered tamper resistant.

In more detail, the present invention provides a tamper-resistant method for authorising access to data between a host and a predetermined number N < M of attached workstations or users, the host including a communications server for managing physical data transmission between the host and M workstations or users; and means for storing access control software and related information; comprising the steps at the host of:

(a) responsive to a service request from a workstation or user, invoking access control software from

Nintendo Exhibit 1003
Part 1 of 2
Page 00519

the storage means and a precomputed list, the list including M station or user identities and an encrypted representation of N indicative of the number of workstations or users authorised access or attachment to the host, the encrypted representation N being formed using an encryption key as a function of the host identity and an offset;

(b) ascertaining the depth N to which the list may be searched by decrypting the representation using the key; and

(c) comparing the identity of the workstation or user originating the service request with the identities of the M stations or users on the list but only to a depth N, and returning an authorisation only upon a match condition.

Such an arrangement is thought to be a tamper-resistant method for controlling the number of users given authorised access to licensed software in a host-based, multiple terminal system. The software expression of such can be embedded among the modules forming a licensed software product.

The above method is based on the unexpected use of an encrypted form of an authorisation list depth parameter. As disclosed hereinafter, access to data is authorised between a host and a predetermined number $N < M$ attached workstations or users. The host includes a communications server for managing physical data transmission between the host and the M workstations or users, and means for storing access control software and related information.

The first operation takes place at the host and includes invoking access control software from the storage means and invoking a precomputed list. These invocations are both in response to a service request from a workstation or user. The list includes M station or user identities and an encrypted representation of the parameter N. $N \leq M$ represents the number of workstations or users authorised access or attachment to the host.

The encryption key is a function of the host identity and an offset. In this regard, an "offset" is a constant that is arithmetically combined with the host identity to obscure the key. For instance, the host identity could be the host serial number hard coded in host memory, or it could be an integer value additively combined thereto.

The second operation involves ascertaining the value of depth parameter N by decrypting the representation using the key. The value N defines the depth to which the list is permitted to be searched.

The third operation requires that the service requester identity be compared with the items of the list to that depth N and an authorisation is returned only if a match condition is found within that depth. Significantly, any change in the search-depth N requires re-encryption thereof.

Advantageously, any host-resident licensed software product, a portion of which being downloadable to accessing terminals, embodying the method of this invention requires only a single installation step, in addition to regulating the number of authorised users. It even permits dynamic authorisation of users to a single machine since the encryption key is a function of the host identity. Note that the use of the host identity limits the use of the code to a predetermined system.

The present invention will be described further by way of example with reference to an embodiment thereof as illustrated in the accompanying drawings, in which:-

Fig. 1 depicts a host CPU-to-workstation download system; and

Figs. 2-5 set out access control list examples 1-4.

Referring now to Fig. 1, there is shown a CPU 1 and a plurality of terminals 17, 19, 21, 23 coupled thereto over paths 9, 11, 13, 15. In the subsequent description, it shall be assumed that the CPU node runs under an operating system that uses a communications server similar to the system described in either "VM/System Product Programmer's Guide to the Server-Requester Programming Interface for VM/System Product" (pp. 6-7), IBM publication SC24-5291-1, December 1986; or "TSO Extensions Programmer's Guide to the Server-Requester Programming Interface for MVS/XA" (pp. 1-3), IBM publication SC28-1309-1, September 1987.

Other computing facility resources are governed by the IBM/370 Principles of Operation as described in Amdahl et al., U.S. Patent 3,400,371, "Data Processing System", issued September 3, 1968.

Referring again to Fig. 1, in addition to a usual complement of operating system services, CPU 1 preferably includes at least one application executable in a communicating relation with at least one terminal over a download interface to an accessing workstation over a designated path. It should be appreciated that licensed software products are expressed in object code only (OCO) form. They are packaged according to a structured program syntax frequently including a plurality of single entrance/single exit modules (see J. E. Nicholls, "The Structure and Design of Programming Languages", The Systems Programming Series, copyright 1975 by Addison-Wesley Publishing Co., Chapter 12, relating to modular programming, especially at page 486). Accordingly, in the preferred embodiment, an access control program (ACP) and an access control list (ACL) are embedded among the product modules. Both the OCO

Nintendo Exhibit 1003
Part 1 of 2
Page 00520

product form and dispersal of the ACP and ACL among several modules should render them relatively immune from isolation and casual inspection.

Access Control List

The ACL preferably comprises a file containing a header record followed by one record per authorised user. The header record will characterise the number of authorised users in the list. For instance, if the header records include an encrypted integer value of three, then only the first three users in the ACL will be authorised to invoke the download transfer operation.

To authorise a user, access must be made to the data set (module) containing the ACL residing in the host CPU 1. At this point, a new authorised ID may be entered consonant with the depth prescribed by the header record. Note that the data set may be protected additionally as described in IBM's Resource Control Facility (RACF) set forth in "OS/VS2 MVS RACF Command Language Reference", IBM publication SC28-0733.

Referring now to Figs. 2-5, there are shown access control list examples 1-4 according to the invention. Fig. 2 lists four names with a parameter depth of N=3. Thus, only the terminal or user identities GEORGE, JOHN, and MARY are authorised, while ROSEALI is not. In Fig. 3, the permitted depth exceeds the length of the list so that another identity could be added. Fig. 4 shows a depth of 1, while Fig. 5 shows a list with a different CPUID. In the latter regard, the depth parameter would not be decrypted since the key is a function of a predetermined CPUID + offset.

As a practical matter, whether the host CPU is local area network or attached to terminals, authorisation and access mechanisms rely principally upon a password match. In the event of mismatch or a repeated pattern of mismatch, entry is merely denied. In other systems, such as the previously mentioned RACF, other criteria such as location or a value of a system clock may be used to control access.

Access Control Program (ACP)

Herein, there is shown one exemplary pseudocode sequence with strong PASCAL overtones, the execution of which embodies the method of the invention. Significantly, the ACP may be called by

ACP(userid: char, encrypt: bool) boolean

the declaration of the ACP program, either once per logged-on session or more than once (e.g., every time a data transfer is intended to be performed), the inputs being defined as

userid - a string of characters defining which userid is to be scanned in the Access Control List (ACL)

encrypt - Boolean variable (TRUE if the ACL header is encrypted, FALSE if the ACL header is decrypted)

ACL - Access Control List

The sequence specifies the following functions including:

(a) Opening the file containing the ACL.

```
Begin
    Reset (ACL)
```

(b) Reading the header record and decoding the depth level N.

```
Read (ACL, header);
If (encrypt) then begin

    max_depth = decrypt (header, get_cpu_id)
End;
```


Nintendo Exhibit 1003
Part 1 of 2
Page 00521

This is implemented by decrypting the header with a key formed from the CPUID + offset according to any well-known encryption/decryption algorithm. Such algorithms are to be found in Ehrsam et al., U.S. Patent 4,227,253, "Cryptographic Communication Security for Multiple Domain Networks", issued October 7, 1980; Matyas et al., U.S. Patent 4,218,738, "Method for Authenticating the Identity of a User of an Information System", issued August 19, 1980; and Meyer and Matyas, "Cryptography - New Dimension in Computer Data Security", copyright 1982 by John Wiley & Sons.

```
        Else begin
             max_depth = header
        End;
```

The depth number is clear in the header.

(c) Scanning the ACL to find a match between the requester ID and the list within the decrypted depth range N.

```
        i = 0;
        Not_found = TRUE;
        While (i < max_depth) and (not_found) do begin
             Readin (ACL_userid)
             IF (ACL_userid = userid) then begin
                  not_found = FALSE;
             End;
             i = i + 1;
        End;
        Return (not_found);
End;
```

(d) If the match is successful - the returned (not_found) = FALSE -, invoke the authorised application on the host. Otherwise - the returned (not_found) = TRUE -, return a message to the requesting workstation indicating UN-AUTHORISED.

It should be noted from the sequence recited, that the two critical structures are the IF..THEN..ELSE conditional statement for ascertaining the depth parameter, followed by the WHILE..DO loop for scanning the ACL for a match condition.

Claims

1. A method for authorising access to application software resident in a CPU host from among N < M workstations or users communicatively attaching the CPU host, comprising the steps of:

(a) forming a list of authorised users and encrypting thereon a depth parameter N, the encryption using a function of the CPU identity and an offset as a key;

(b) responsive to each application software access request from among the workstations or users, accessing the list and decrypting the depth parameter N with the key; and

(c) scanning the list within the depth N and returning an access authorisation to the requester only upon an identity match.

2. A method as claimed in claim 1, wherein the access authorisation is of the form of invocation of the application software, and the refusal of the access request is of the form of a message sent to the requesting workstation or user.

3. A method as claimed in either preceding claim, wherein the arrangement of the CPU host communicatively attaching the workstations or users is selected from the set consisting of a local area

Nintendo Exhibit 1003
Part 1 of 2
Page 00522

network and a multiprogramming, multiprocessing system exemplified by VM.

4. A method as claimed in any preceding claim, wherein the method steps further include modifying the search depth N only by re-encrypting same.

5. A method as claimed in any preceding claim, wherein the list and the access control software embodying the method are embedded within an object-coded version of the application.

6. A tamper-resistant method for authorising access to data between a host and a predetermined number N < M of attached workstations or users, the host including a communications server for managing physical data transmission between the host and M workstations or users; and means for storing access control software and related information; comprising the steps at the host of:

(a) responsive to a service request from a workstation or user, invoking access control software from the storage means and a precomputed list, the list including M station or user identities and an encrypted representation of N indicative of the number of workstations or users authorised access or attachment to the host, the encrypted representation N being formed using an encryption key as a function of the host identity and an offset;

(b) ascertaining the depth N to which the list may be searched by decrypting the representation using the key; and

(c) comparing the identity of the workstation or user originating the service request with the identities of the M stations or users on the list but only to a depth N, and returning an authorisation only upon a match condition.

7. A method as claimed in claim 6, wherein the method steps further include modifying the search depth N only by re-encrypting same.

Nintendo Exhibit 1003
Part 1 of 2
Page 00523

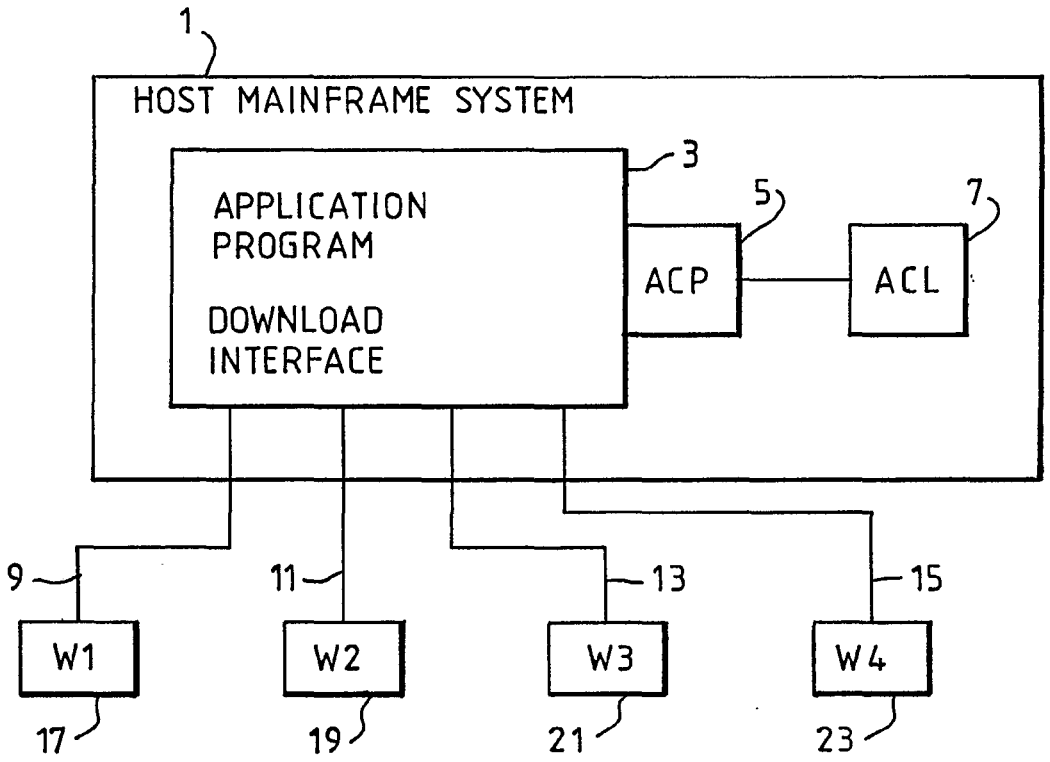


Fig. 1

Nintendo Exhibit 1003
Part 1 of 2
Page 00524

ACL-1

```
-ENCRYPTED VALUE OF 3 WITH SEED=CPUID-
GEORGE        /* USER 1, E.G., W1, IN FIGURE 1 */
JOHN          /* USER 2, E.G., W2, IN FIGURE 1 */
MARY          /* USER 3, E.G., W3, IN FIGURE 1 */
ROSEALI       /* USER 4, E.G., W4, IN FIGURE 1 */
```

ACCESS CONTROL LIST, EXAMPLE 1

Fig. 2

ACL-2

```
-ENCRYPTED VALUE OF 5 WITH SEED=CPUID-
GEORGE        /* USER 1, E.G., W1, IN FIGURE 1 */
JOHN          /* USER 2, E.G., W2, IN FIGURE 1 */
MARY          /* USER 3, E.G., W3, IN FIGURE 1 */
ROSEALI       /* USER 4, E.G., W4, IN FIGURE 1 */
```

ACCESS CONTROL LIST, EXAMPLE 2

Fig. 3

ACL-3

```
1
GEORGE        /* USER 1, E.G., W1, IN FIGURE 1 */
JOHN          /* USER 2, E.G., W2, IN FIGURE 1 */
MARY          /* USER 3, E.G., W3, IN FIGURE 1 */
ROSEALI       /* USER 4, E.G., W4, IN FIGURE 1 */
```

ACCESS CONTROL LIST, EXAMPLE 3

Fig. 4

ACL-4

```
-ENCRYPTED VALUE OF 3 WITH SEED=A DIFFERENT CPUID THAN THE HOST-
GEORGE        /* USER 1, E.G., W1, IN FIGURE 1 */
JOHN          /* USER 2, E.G., W2, IN FIGURE 1 */
MARY          /* USER 3, E.G., W3, IN FIGURE 1 */
ROSEALI       /* USER 4, E.G., W4, IN FIGURE 1 */
```

ACCESS CONTROL LIST, EXAMPLE 4

Fig. 5

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 July 2003 (31.07.2003)

PCT

(10) International Publication Number
WO 03/063524 A1

(51) International Patent Classification[7]: H04Q 7/20, H04L 9/32

(21) International Application Number: PCT/US03/01572

(22) International Filing Date: 16 January 2003 (16.01.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/057,735 22 January 2002 (22.01.2002) US

(71) Applicant: YAHOO. INC. [US/US]; 701 First Avenue, Sunnyvale, CA 94089 (US).

(72) Inventors: TZAN-EN SZETO, Christopher; 5230 War Wagon Drive, San Jose, CA 95136 (US). PATWARDHAN, Chintamani; 898 Persimmon Avenue, Sunnyvale, CA 94087 (US). TORGEMANE, Henri; 2249 Mclaughlin Avenue #1, San Jose, CA 95122 (US).

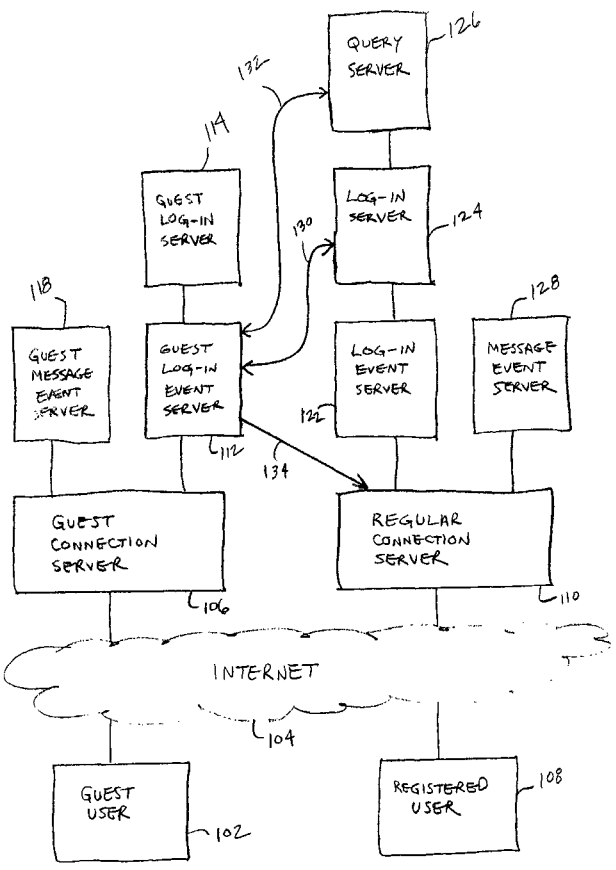
(74) Agent: JAMES, William, J.; Van Pelt & Yi LLP, Suite 200, 10050 N. Foothill Boulevard, Cupertino, Ca 95014 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI,

[Continued on next page]

(54) Title: PROVIDING INSTANT MESSAGING FUNCTIONALITY IN NONINSTANT MESSAGING ENVIRONMENTS



(57) Abstract: A system and method are disclosed for enabling a guest user (102) who is not a registered user of an instant messaging system to communicate by instant messaging with a registered user (108) of the system. An indication that the guest user desires to communicate with the registered user by instant messaging is received. Browser-executable computer code comprising computer instructions for providing at least limited instant messaging functionality to the guest user at the guest user's client computer system, without requiring the guest user to download and install client side instant messaging application software and without requiring the guest user to register as a user of the instant messaging system, is sent to the guest user's client computer system. An instant messaging session between the guest user and the registered user is facilitated.

WO 03/063524 A1

SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search 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.

PROVIDING INSTANT MESSAGING FUNCTIONALITY IN NON-INSTANT MESSAGING ENVIRONMENTS

Field of the Invention

The present invention relates generally to instant messaging. A system and method for providing instant messaging functionality in a non-instant messaging environment is disclosed.

Background Of The Invention

Instant messaging technology enables two or more participants to communicate via a computer network, such as the Internet, in more or less real time. Typically, each participant uses a client computer system to send and receive messages. Each client computer system typically is connected via a network to an instant messaging connection server. The connection server receives and processes messages from participants, including by forwarding them to the client systems of the other participants for display. The connection server may also be configured to send messages on behalf of the system, such as to inform participants that a fellow participant has disconnected or logged off.

Typically, instant messaging application software is installed at each client system to enable the client system to be used as an instant messaging client. The instant messaging software may be made available for download, for example, from a web page accessible via the Internet. A user invokes this software on the client system in order to communicate by instant messaging with one or more other participants. The client side application software typically establishes a connection between the client system and the

Nintendo Exhibit 1003
Part 1 of 2
Page 00528

connection server and either automatically logs the user into the connection server or prompts the user to enter the information necessary to log in, such as a user name and password. The user may then communicate by means of instant messaging with one or more other users who are logged into the instant messaging system at that time.

Under this approach, only users who have downloaded or otherwise installed the client side instant messaging software that enables them to connect to the same instant messaging system may communicate with each other. Moreover, typically the process of downloading or otherwise installing the client side instant messaging application software includes a registration process in which the user registers as a user of the system by establishing a user name and account. This process requires time to complete, which discourages some potential new users from registering and downloading the required software. As a result, instant messaging users are typically limited to communicating by instant messaging only with other users who have registered with and downloaded the client side software provided by the particular instant messaging service provider with whom they have registered and whose client side software they have installed. If a user of such a system wishes to communicate by instant messaging with someone who is not a registered user of that system, the user typically must ask the individual with whom he wishes to communicate to download or otherwise obtain the software and register as a user in order to be able to do so.

Therefore, there is a need for a way to enable an instant messaging user to communicate by instant messaging with a person who has neither downloaded or otherwise installed the client side instant messaging application software normally required for such communication nor registered and logged in as a registered user of the

Nintendo Exhibit 1003
Part 1 of 2
Page 00529

instant messaging system. There also is a need for a way for such a user to invite someone who may or may not be a registered user of the particular instant messaging system used by the user to communicate with the user by instant messaging. There is also a need to provide instant messaging functionality to a client system without requiring that client side application software be downloaded and installed, and without requiring that a person register as a user before communicating. Finally, there is a need to enable a guest user who is not a registered user to connect to and communicate through use of an instant messaging connection server.

Summary Of The Invention

A system and method for providing instant messaging functionality in a non-instant messaging environment is disclosed. A guest user indicates his or her interest in communicating through instant messaging. The guest user is connected to a connection server and assigned a temporary user identification. The guest user uses this temporary identification to communicate by instant messaging with a registered user of the instant messaging system.

It should be appreciated that the present invention can be implemented in numerous ways, including as a process, an apparatus, a system, a device, a method, or a computer readable medium such as a computer readable storage medium or a computer network wherein program instructions are sent over optical or electronic communication links. Several inventive embodiments of the present invention are described below.

A method for enabling a guest user who is not a registered user of an instant messaging system to communicate by instant messaging with a registered user of the

Nintendo Exhibit 1003
Part 1 of 2
Page 00530

system is disclosed. In one embodiment, an indication that the guest user desires to communicate with the registered user by instant messaging is received. Browser-executable computer code comprising computer instructions for providing at least limited instant messaging functionality to the guest user at the guest user's client computer system, without requiring the guest user to download and install client side instant messaging application software and without requiring the guest user to register as a user of the instant messaging system, is sent to the guest user's client computer system. An instant messaging session between the guest user and the registered user is facilitated.

A system for enabling a guest user who is not a registered user of an instant messaging system to communicate by instant messaging with a registered user of the system is disclosed. In one embodiment, the system comprises a web server and an instant messaging server. The web server is configured to receive an indication that the guest user desires to communicate with the registered user by instant messaging and send to a client computer system associated with the guest user browser-executable computer code comprising computer instructions for providing at least limited instant messaging functionality to the guest user at the client computer system, without requiring the guest user to download and install client side instant messaging application software and without requiring the guest user to register as a user of the instant messaging system. The instant messaging server is configured to facilitate an instant messaging session between the guest user and the registered user. In other embodiments, the web server and/or instant messaging server may comprise a plurality of servers.

Nintendo Exhibit 1003
Part 1 of 2
Page 00531

These and other features and advantages of the present invention will be presented in more detail in the following detailed description and the accompanying figures, which illustrate by way of example the principles of the invention.

Brief Description Of The Drawings

The present invention will be readily understood by the following detailed description in conjunction with the accompanying drawings, wherein like reference numerals designate like structural elements, and in which:

Figure 1A is a schematic diagram illustrating an instant messaging system used in one embodiment to provide instant messaging functionality in a non-instant messaging environment.

Figure 1B shows the system components illustrated in Figure 1A with the same reference numerals being used in Figure 1B as in Figure 1A to indicate like components.

Figure 2 is a flowchart illustrating a process used in one embodiment to provide instant messaging functionality in a non-instant messaging environment.

Figure 3 is an illustration of an electronic mail message composition page 300 that may be used in one embodiment to request that an HTML messenger toolbox be incorporated in an outgoing electronic mail message.

Figure 4 is an illustration of an HTML messenger toolbox 400 used in one embodiment as an entry point to enable an invited user to communicate with a registered instant messaging user by means of an instant messaging system that would have otherwise have required the invited user to download and install client side instant

Nintendo Exhibit 1003
Part 1 of 2
Page 00532

messaging application software and to register as an instant messaging user, if the invited user had not previously done so.

Figure 5 is an illustration of an exemplary electronic mail message comprising an instant messaging toolbox such as the HTML messenger toolbox illustrated in Figure 4.

Figure 6 is a flowchart illustrating the processes executed in one embodiment at the client system of an invited user of an instant messaging system to enable the invited user to initiate an instant messaging session.

Figure 7 is an illustration of a log in page used in one embodiment to obtain a display name to be used for the invited user in an instant messaging session to be established between the invited user, logging in as a guest user, and the inviting instant messaging user associated with the HTML messenger toolbox.

Figure 8 is a flowchart of a process executed in one embodiment at the instant messaging connection server to process a request from an invited user to log in as a guest user, as in step 204 of Figure 2.

Figure 9 is a flowchart illustrating a process executed in one embodiment by the browser-executable client at the invited user's client system to send and receive instant messages between the invited user and the registered user associated with the HTML messenger toolbox when the invited user has logged in as a guest user.

Figure 10 is an illustration of an exemplary guest user instant messaging user interface display 1000 provided to a guest user in one embodiment, as in step 906 of Figure 9.

Nintendo Exhibit 1003
Part 1 of 2
Page 00533

Figure 11 is a flowchart illustrating a process used in one embodiment at the guest message server to process instant messages sent by a guest user. In step 1102, a message from the guest user to the inviting user is received at the connection server.

Figure 12 is an illustration of an instant messaging display 1200 used in one environment to provide an instant messaging user interface to a registered instant messaging user for an instant messaging session with a guest user that is not a registered instant messaging user.

Figure 13 is a flowchart illustrating a process used in one embodiment to process at the connection server instant messages sent from a registered instant messaging user to a guest user.

Figure 14 is a flowchart illustrating a process used in one embodiment to process, at the connection server an indication that either the guest user or the inviting user has logged off, as in step 208 of the process shown in Figure 2.

Detailed Description

A detailed description of a preferred embodiment of the invention is provided below. While the invention is described in conjunction with that preferred embodiment, it should be understood that the invention is not limited to any one embodiment. On the contrary, the scope of the invention is limited only by the appended claims and the invention encompasses numerous alternatives, modifications and equivalents. For the purpose of example, numerous specific details are set forth in the following description in order to provide a thorough understanding of the present invention. The present

Nintendo Exhibit 1003
Part 1 of 2
Page 00534

invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the present invention is not unnecessarily obscured.

Figure 1A is a schematic diagram illustrating an instant messaging system used in one embodiment to provide instant messaging functionality in a non-instant messaging environment. An invited user client system 102 is connected via the Internet 104 with a guest connection server 106. In one embodiment, an invited user who is not a registered user of the instant messaging system may access and use the instant messaging system as a guest user by connecting to the guest connection server 106 to communicate by instant messaging with a registered instant messaging user, as described more fully below. As used herein, an "invited user" is one who has been invited to communicate by instant messaging with the registered instant messaging user who extended the invitation, as described more fully below. A user may be an "invited user" even if the entry point accessed by the user to initiate communication by instant messaging with the registered user who extended the invitation was not specifically directed to that user (e.g., the entry point was posted on a web page accessible by the user and other users). A registered user client system 108, such as may be used by the user who invited the invited user to communicate by instant messaging (referred to herein as the "inviting user"), is connected via the Internet 104 with a regular connection server 110.

The guest connection server 106 is connected to a guest login event server 112. In one embodiment, when an invited user indicates a desire to log in as a guest user, as opposed to as a registered user, the invited user is prompted to supply a display name and

Nintendo Exhibit 1003
Part 1 of 2
Page 00535

is given an opportunity to enter an initial message, as described more fully below in connection with Figures 3, 4, and 6. In one embodiment, a login request message comprising the display name and initial message entered by the guest user is sent from the guest user client system 102 to the guest connection server 106. Upon receipt, the login request message is forwarded to the guest login event server 112 for processing.

In one embodiment, a request to login as a guest user is only further processed if it is determined that the target registered instant messaging user with whom the guest user wishes to communicate by instant messaging (i.e., the inviting user) is logged into the instant messaging system and available to send and receive instant messages. In one embodiment, a registered user logs in by connecting to the instant messaging system via a connection server such as regular connection user 110. The regular connection server 110 is connected to a login event server 122. A request from a registered user to login is directed to a regular connection server such as regular connection server 110, which passes the request to log in to the login event server 122 for processing. In one embodiment, the login event server 122 is connected to a user profile database, not shown in Figure 1A, which contains information concerning the registered user, such as the registered user's system preferences and data associated with the user, such as a buddy list (described below). In one embodiment, the login event server 122 uses data from the user profile database to process the request of a registered user to log in.

The login event server 122 is connected to a login server 124. In one embodiment, the login event server 122 sends a request to the login server 124 to establish a record within the login server 124 indicating that the registered user is logged in and comprising information to be used to deliver instant messages to the registered

Nintendo Exhibit 1003
Part 1 of 2
Page 00536

user, such as the IP address of the connection server through which the registered user has established a connection with the system and the port number being used on the connection server to communicate with the registered user's client system.

The login server 124 is connected to a query server 126. In one embodiment, the query server 126 handles routine requests for connection information regarding the registered users currently logged in to the system. In one embodiment, a copy of the record established for a registered user in the login server 124 upon login is sent to the query server 126 at the time of login and is deleted from the query server 126 and the login server 124 when the registered user logs off. In one embodiment, the record in login server 124 associated with a particular registered user may be updated more frequently during the time during which the registered user is logged in, but the query server 126 does not receive each such update so long as the update does not affect the identification and connection information associated with the registered user.

Returning to consideration of the log in process for a guest user, when the guest login event server 112 receives a request to log in as a guest user, it assigns to the guest user a randomly generated guest user identification. The guest login event server then queries the query server 126 via a connection 132 to verify that the target registered user with whom the guest user has indicated a desire to communicate by instant messaging is logged in. The connection 132 may be a physical connection, such as a cable, or a logical connection, such as a network or other connection that enables the two servers to exchange data. In one embodiment, if the registered user is not logged in, the request to log in as a guest user is not further processed and an error message is returned to the guest user.

Nintendo Exhibit 1003
Part 1 of 2
Page 00537

The guest login event server 112 is connected to a guest login server 114. If the guest login event server determines that the registered user is logged in, the guest login event server 112 sends a request to the guest login server 114 to establish a login record for the guest user in the guest login server 114. In one embodiment, the record indicates that the guest user is logged in, associates the guest user identification with the guest user, and comprises information needed to deliver an instant message to the guest user, such as the IP address of the guest connection server through which the guest user has connected to the system and the port number being used on the guest connection server to communicate with the guest user's client system.

The guest login event server 112 is connected to the query server 126 by connection 132. The connection 132 may be a physical connection, such as a cable, or a logical connection, such as a network or other connection that enables the two servers to exchange data. In one embodiment, preparatory to sending the initial message included in the guest user's request to log in, the guest login event server 112 queries the query server 126 via connection 132 to obtain the connection information needed to deliver the initial message to the target registered user for whom it is intended. In one embodiment, the information so obtained from the query server 126 comprises the IP address of the connection server through which the registered user is connected to the instant messaging system and the port number being used by the connection server to communicate with the target registered user's client system.

The guest login event server 112 is connected to the regular connection server 110 via connection 134. The connection 134 may be a physical connection, such as a cable, or a logical connection, such as a network or other connection that enables the two

Nintendo Exhibit 1003
Part 1 of 2
Page 00538

servers to exchange data. In one embodiment, once the guest login event server 112 has obtained from the query server 126 the connection information for the target registered user, the guest login event server 112 uses that information to send the initial message included in the guest user's login request to the target registered user via connection 134 and regular connection server 110.

The guest connection server 106 is connected to a guest message event server 118, which processes subsequent messages received from the guest user as described below in connection with Figure 1B. The regular connection server 110 is connected to a message event server 128, which processes messages received from the registered user as described below in connection with Figure 1B.

In one embodiment, the respective functions of the guest connection server and the regular connection server are performed by a single connection server and no separate or dedicated connection server is provided to handle guest users. In one embodiment, the guest connection server 106 shown in Figure 1A may be one of a plurality of guest connection servers, each configured to provide the functionality described as being provided by the guest connection server 106. In one embodiment, the regular connection server 110 shown in Figure 1A may be one of a plurality of connection servers, each configured to provide the functionality described as being provided by the regular connection server 110. In one embodiment, all of the functions described above are performed by a single system, without providing separate systems or modules to provide the functionality described above. The functionality described above may be divided among one or more systems in the manner described above or in any number of different

Nintendo Exhibit 1003
Part 1 of 2
Page 00539

combinations, depending on the needs and resources available in any particular implementation.

The schematic diagram in Figure 1A does not show all of the logical or other connections between the components associated primarily with the guest user (comprising elements 102, 106, 112, 114, and 118), on the one hand, and the components associated primarily with the registered user (comprising elements 108, 110, 122, 124, 126, and 128), on the other hand, and instead shows only those logical or other connections involved in the processing of logging in and sending the initial message from the guest user to the registered user. The sending and receipt of subsequent messages is discussed immediately below in connection with Figure 1B.

Figure 1B shows the system components illustrated in Figure 1A with the same reference numerals being used in Figure 1B as in Figure 1A to indicate like components. The relative position of certain of the components has been changed to facilitate the clear illustration of certain connections relevant to the processing of messages sent by an invited user to an inviting user subsequent to the initial message included with the invited user's login request, as described above, and messages sent from the inviting user to the invited user. As in Figure 1A, not all logical or other connections between components associated primarily with the invited user, on the one hand, and components associated primarily with the inviting user, on the other hand, are shown in Figure 1B. Instead, only those connections are shown that play a role in the sending of messages from the invited user to the inviting user (subsequent to the initial message) or the sending of messages from the inviting user to the invited user.

Nintendo Exhibit 1003
Part 1 of 2
Page 00540

To send an instant message to an invited who is not a registered user of the instant messaging system, and who has therefore logged in as a guest user, the inviting user enters the message in the message entry area of an instant messaging window displayed at the registered user client system 108 and selects a "send" option. The client side instant messaging application program installed on the registered user client system 108 sends the message to the regular connection server 110 via the Internet 104. The regular connection server 110 passes the message to the message event server 128 for processing. The message event server 128 queries the guest login server 114 via a connection 160 to obtain connection information necessary to deliver the message to the guest user. The connection 160 may be a physical connection, such as a cable, or a logical connection, such as a network or other connection that enables the two servers to exchange data. In one embodiment, if connection information is not available from the guest login server 114, the message event server 128 is configured to recognize that the guest user is no longer logged in and returns an error message to the registered user indicating that the message could not be delivered because the guest user has logged off.

If the message event server 128 successfully obtains connection information for the guest user, the message event server uses the connection information to deliver the message to the guest user via a connection 162 to the guest connection server 106. The connection 162 may be a physical connection, such as a cable, or a logical connection, such as a network or other connection that enables the two servers to exchange data. The message is then delivered by the guest connection server 106 to the invited user client system 102 via the Internet 104, and is displayed to the guest user at the invited user client system 102.

Nintendo Exhibit 1003
Part 1 of 2
Page 00541

To send a subsequent message (i.e., subsequent to the initial message included with the guest user's login request) to the inviting user, the guest user enters the message in a message entry area displayed at the invited user client system 102. In one embodiment, the instant messaging user interface displayed at the invited user client system 102 is provided by a browser-executable instant messaging client, as described more fully below. The invited user client system 102 sends the message to the guest connection server 106 via the Internet 104. The guest connection server passes the message to the guest message event server 118 for processing. The guest message event server 118 queries the query server 126, via a connection 164, to obtain connection information necessary to deliver the message to the registered user. The connection 164 may be a physical connection, such as a cable, or a logical connection, such as a network or other connection that enables the two servers to exchange data.

In one embodiment, if connection information is not available from the query server 126, the guest message event server 118 is configured to recognize that the inviting user is no longer logged in and returns an error message to the guest user indicating that the message could not be delivered because the registered user has logged off.

If the guest message event server 118 successfully obtains connection information for the inviting user, the guest message event server uses the connection information to deliver the message to the inviting user via a connection 166 to the regular connection server 110. The connection 166 may be a physical connection, such as a cable, or a logical connection, such as a network or other connection that enables the two servers to exchange data. The message is then delivered by the regular connection server 110 to the

Nintendo Exhibit 1003
Part 1 of 2
Page 00542

registered user client system 108 via the Internet 104, and is displayed to the registered user at the registered user client system 108.

Figure 2 is a flowchart illustrating a process used in one embodiment to provide instant messaging functionality in a non-instant messaging environment. The process begins at step 202 in which a request to incorporate an instant messenger toolbox comprising computer code written in the hyper text markup language (HTML) is received. In one embodiment, as described more fully below, such an indication may be received from a user composing an electronic mail message. In one embodiment, a request may be received to incorporate an HTML messenger toolbox and any web page, message, or other electronic document that is based on or supports HTML. In one alternative embodiment, the toolbox is provided using computer code written in a computer programming language other than HTML. Any computer code that is executable by application software associated with the electronic communication or other document in which the toolbox is embedded may be used.

Figure 3 is an illustration of an electronic mail message composition page 300 that may be used in one embodiment to request that an HTML messenger toolbox be incorporated in an outgoing electronic mail message. In one embodiment, if requested the toolbox is included in the outgoing electronic mail message when the message is sent to the recipient to whom it is addressed. The electronic mail message composition page 300 comprises a "to" field 302, a "subject" field 304, and a "cc:" field 306 in which addressing and subject information for the electronic mail message may be entered by the user composing the message. The composition page 300 further includes a “send” button 308 to be used by the user composing the message to indicate that the message is

Nintendo Exhibit 1003
Part 1 of 2
Page 00543

complete and ready to be sent to the recipient(s) to whom it is addressed. The message composition page 300 also includes a "cancel" button 310 which may be used to cancel a request to prepare and send an electronic mail message and to exit the electronic mail composition page. The electronic mail message composition page 300 further comprises a message text entry area 312, which may be used by the user composing the message to enter the text of the message. The electronic mail message composition page 300 further includes an instant messenger toolbox insertion request check box 314. In one embodiment, when the check box 314 is selected, a check mark appears in the box (as shown in Figure 3) and a toolbox preview image 316 is displayed in the message text entry area 312. In one embodiment, an image of the messenger toolbox, as it will appear in the message when sent, is displayed in the message text area 312 to show the user composing the message how the toolbox will appear when displayed to the recipient as part of the message. In one embodiment, an image of the toolbox as opposed to the actual HTML toolbox itself is inserted in the mail message composition page to prevent the user composing the message from inadvertently altering the HTML code that will be used to provide the toolbox as part of the message as received. If the check box 314 is not selected, or is de-selected, no check mark appears in the check box and no toolbox preview image appears in the message text entry area 312.

Figure 4 is an illustration of an HTML messenger toolbox 400 used in one embodiment as an entry point to enable an invited user to communicate with a registered instant messaging user by means of an instant messaging system that would have otherwise have required the invited user to download and install client side instant messaging application software and to register as an instant messaging user, if the invited

Nintendo Exhibit 1003
Part 1 of 2
Page 00544

user had not previously done so. An image of an HTML messenger toolbox such as the messenger toolbox 400 shown in Figure 4 would be displayed, if requested by the inviting user, in one embodiment in the toolbox preview image display area 316 of Figure 3. The exemplary HTML messenger toolbox 400 comprises an inviting instant messaging user information display area 402. In one embodiment, as shown in Figure 4, the inviting instant messaging user information area 402 comprises a user name or identification for the inviting user. In the example shown in Figure 4, the inviting instant messaging user is identified as "sender", which in this example refers to the sender of an electronic mail message such as might be sent through use of an electronic message composition page such as the electronic mail message composition page 300 of Figure 3. The inviting instant messaging user information area 402 further comprises an on line presence indicator 404. In one embodiment, the on line presence indicator 404 is used to signal to a recipient or other viewer of the HTML messenger toolbox whether or not the inviting instant messaging user associated with the toolbox is presently signed in to the instant messaging system, thereby making it possible for the person viewing the HTML messenger toolbox to communicate with the inviting instant messaging user at the present time through instant messaging. The HTML messenger toolbox 400 further comprises an on line presence indicator key display area 406 in which a key to the on line presence indicators is provided. In the example shown in Figure 4, a smiling face indicator indicates that the inviting instant messaging user associated with the HTML messenger toolbox is on line and signed in to the instant messaging system, and an image of a face that suggests sleep, with flat horizontal lines representing the eyes and mouth, is used to indicate that the inviting instant messaging user associated with the HTML messenger

Nintendo Exhibit 1003
Part 1 of 2
Page 00545

toolbox is off line and is not available to participate in an instant messaging session. The exemplary HTML messenger toolbox 400 shown in Figure 4 further comprises an initial message text entry area 408 in which an individual wishing to communicate with the inviting instant messaging user associated with the HTML messenger toolbox may enter an initial message to the inviting user. The HTML messenger toolbox 400 also comprises a "send" button 410. In one embodiment, selection of the "send" button 410 causes a browser pop up window to open and be connected via the Internet to a web page comprising computer code written in one or more browser-executable programming languages to provide limited instant messaging functionality, as described more fully below.

Figure 5 is an illustration of an exemplary electronic mail message comprising an instant messaging toolbox such as the HTML messenger toolbox illustrated in Figure 4. The electronic mail message display 500 comprises a header information display area 502 in which address information and subject matter information may be displayed. The message display 500 further comprises a "reply" button 504 which may be used by the recipient of the message to send a reply electronic mail message to the sender of the original message by opening an electronic mail message composition page or display that is pre-addressed to the sender of the original message. The message display 500 further comprises a "delete" button 506 which may be used by the recipient to delete the electronic mail message from the recipient's in box. The message display 500 further comprises a message text display area 508 in which the text of the sender's message is displayed. In one embodiment, if the sender of the message (i.e., the inviting user) has indicated that an instant messaging toolbox such as the HTML messenger toolbox

Nintendo Exhibit 1003
Part 1 of 2
Page 00546

described above should be included with the message as delivered to the recipient, an instant messaging toolbox 510 is provided as part of the message and displayed within the message text display area 508. In one embodiment, the instant messaging toolbox 510 is the HTML messenger toolbox 400 described above and illustrated in Figure 4.

Returning to the process illustrated in Figure 2, the process continues with step 204 in which a request to log in as a guest user of the instant messaging system is received and processed. In one embodiment, as described above, the HTML messenger toolbox is used by a would be guest user of the instant messaging system to indicate that the guest user wishes to communicate by instant messaging with the registered instant messaging user associated with the messenger toolbox, as described more fully below.

In step 206 of the process shown in Figure 2, instant messages from the guest user to the registered user and instant messages from the registered user to the guest user are received by the instant messaging system and processed. In one embodiment, the processing includes delivery of the instant messaging message to the intended recipient. The receipt and processing of instant messages is described more fully below in connection with Figures 11 and 13.

In step 208 of the process shown in Figure 2, an indication that one of the participants has logged off is received and processed. In one embodiment, the instant messaging system receives such an indication if a participant either selects a "sign off" button or option in the participant's instant messaging display window or if the participant closes the participant's instant messaging display window. In one embodiment, a registered user does not sign off when he or she closes an instant messaging window associated with a particular instant messaging session (or "conversation"), and such a

Nintendo Exhibit 1003
Part 1 of 2
Page 00547

user must instead take other steps to sign off. In one embodiment, the processing performed in step 208 comprises informing the other participant(s) that a participant has logged off. The processing performed in step 208 is described more fully below in connection with Figure 14.

In step 210 of the process shown in Figure 2, the instant messaging session between the guest user and the registered user is terminated and the temporary guest user ID assigned to the guest user is discarded and no longer associated with the guest user. The process shown in Figure 2 ends in step 212.

Figure 6 is a flowchart illustrating the processes executed in one embodiment at the client system of an invited user of an instant messaging system to enable the invited user to initiate an instant messaging session. The process begins with step 602 in which an indication is received from the user that the user wishes to communicate by instant messaging. At the invited user's client system, this indication is received in one embodiment by an HTML messenger toolbox, such as the HTML messenger toolbox described above and illustrated in Figure 4. In one embodiment, the indication is received upon selection of the invited user of a "send" button such as the "send" button 410 of Figure 4.

In step 604 of the process shown in Figure 6 the message text of the initial message entered by the invited user is received and stored locally. In one embodiment, the initial message text is the text entered by the invited user in an initial message text entry area, such as the initial message text entry area 408 of Figure 4.

In one embodiment, upon completion of steps 602 and 604, the HTML messenger toolbox causes a browser pop up window to open and to be connected via the Internet to

Nintendo Exhibit 1003
Part 1 of 2
Page 00548

an instant messaging client page configured to provide limited instant messaging functionality, as described more fully below. In one embodiment, the instant messaging client page comprises a browser-executable instant messaging client. In one embodiment, the browser-executable instant messaging client is provided at least in part by computer code written in the Dynamic HyperText Markup Language (DHTML). In one embodiment, DHTML is used to control the layout and appearance of the browser-executable instant messaging client, JavaScript is used to manipulate the HTML dynamically, and a Java Applet is used to manage the network interface. In other embodiments, other programming languages and tools may be used. In one embodiment, for example, the instant messaging functionality described herein may be provided by a browser-executable instant messaging client implemented using JavaScript and HTTP. In one embodiment, ActiveX is used. In such an embodiment, the ActiveX control must be downloaded and installed by the guest user before the instant messaging client may be used. In one embodiment, Flash is used in conjunction with an XML stream.

In one embodiment, in step 606 of the process shown in Figure 6, the browser-executable instant messaging client checks to determine if the client side instant messaging application software is installed on the invited user's client system. In one embodiment, JavaScript code is used by the instant messaging client to determine if the instant messaging software is installed.

In step 608, it is determined if the client side instant messaging application software has been found on the invited user's client system. If the client side instant messaging application software has been found on the client system, the process proceeds to step 610 in which the installed client side instant messaging application software is

Nintendo Exhibit 1003
Part 1 of 2
Page 00549

invoked to enable the invited user to sign in as a registered user and communicate with the invited user associated with the HTML messenger toolbox in a regular instant messaging session. In one embodiment, the user name or identification of the inviting user associated with the HTML messenger toolbox is passed to the invited user's installed client side instant messaging application software to enable the software to establish an instant messaging session with the inviting user associated with the instant messenger toolbox. In one embodiment, the initial message entered by the invited user in the message text entry area of the HTML messenger toolbox is passed to the installed client side instant messaging application software to enable that text to be passed as an initial message to the inviting user associated with the HTML messenger toolbox in the regular instant messaging session that will be initiated by the installed instant messaging application software. If the instant messaging application software for the instant messaging system is found to be installed on the client system of the invited user, the invited user logs in not in the manner described above for a "guest user", but rather as a registered user, like the inviting user.

If it is determined in step 608 that the client side instant messaging application software has not been found on the invited user's client system, the process proceeds to step 614 in which the browser-executable instant messaging client displays a streamlined login page to the invited user to enable the invited user to log in as a guest user.

Figure 7 is an illustration of a log in page used in one embodiment to obtain a display name to be used for the invited user in an instant messaging session to be established between the invited user, logging in as a guest user, and the inviting instant messaging user associated with the HTML messenger toolbox. The exemplary log in

Nintendo Exhibit 1003
Part 1 of 2
Page 00550

page 700 comprises an inviting user identification display area 702 in which information identifying the inviting user associated with the HTML messenger toolbox is displayed. In the example shown in Figure 7, the user name "sender" is displayed in the display area 702, indicating that "sender" is the inviting instant messaging user associated with the HTML messenger toolbox invoked by the guest user. As shown in Figure 7, in one embodiment the login display 700 comprises instructions to the guest user on how to establish the instant messaging session. The login display 700 further comprises a display name entry area 704 to be used by the guest user to enter a display name by which the guest user will be identified to the other participant(s) in the instant messaging session. The login display 700 further comprises a "submit" button 706, which the guest user may select after entering a display name to submit the display name to the instant messaging connection server for processing.

Referring further to Figure 6, in step 616 login data is received and forwarded to the instant messaging connection server. In one embodiment, the log in page shown in Figure 7 is used and the login data entered by the guest user is received by the browser-executable instant messaging client and forwarded by the browser-executable instant messaging client to the instant messaging connection server upon selection of the submit button 706 by the guest user.

In one embodiment, the instant messaging system is associated with a broader subscriber-based system in which some but not all of the subscribing users have downloaded and installed the client side instant messaging application software and have registered as instant messaging users. In one embodiment, subscribers may sign in to the on line service for purposes of receiving other services such as electronic mail and

Nintendo Exhibit 1003
Part 1 of 2
Page 00551

personalized calendar, news, and/or other services. In one such embodiment, the process shown in Figure 6 is modified such that prior to sending a guest user to a log in page, as in step 614 of the process shown in Figure 6, the browser-executable client checks to see if the guest user is a subscriber to the on line service who has not installed the instant messaging software associated with the on line service but who has subscribed to and is presently signed in to the broader on line service. In one such embodiment, if it is determined that the guest user has signed to the broader on line service, the user and/or display name associated with the subscriber is used as the guest user's display name for purposes of the instant messaging session to be established with the registered instant messaging user associated with the HTML messenger toolbox and step 614 of Figure 6 is omitted.

In one alternative embodiment, the guest user is not prompted to provide a display name and the temporary user identification assigned by the connection server, as described more fully below, is used to identify the guest user. In such an embodiment, steps 614 and 616 of Figure 6 are omitted and the browser-executable client merely requests a temporary guest user identification from the connection server, without prompting the guest user to provide a display name, if it is determined that the instant messaging application software is not installed on the guest user's client system.

Figure 8 is a flowchart of a process executed in one embodiment at the instant messaging connection server to process a request from an invited user to log in as a guest user, as in step 204 of Figure 2. In step 802, the connection server receives a request to log in as a guest user and communicate by instant messaging with an inviting instant messaging user. In one embodiment, the request comprises an identification of the client

Nintendo Exhibit 1003
Part 1 of 2
Page 00552

system being used by the guest user. In one embodiment, the identification comprises an Internet protocol (IP) address and port number associated with the client system being used by the guest user. In one embodiment, the request further comprises an identification of the inviting instant messaging user associated with the HTML toolbox initially invoked by the guest user. In one embodiment, the request comprises a display name entered by the guest user in a display name entry area such as entry area 704 of Figure 7. In one embodiment, the request to log in is sent by the browser-executable client to the connection server.

In step 804 of the process shown in Figure 8, it is determined whether the inviting instant messaging user is currently logged in to the instant messaging system. If it is determined in step 804 that the inviting instant messaging user is not logged in to the instant messaging system, the process proceeds to step 806 in which an error message is returned to the client system being used by the guest user and the guest user is disconnected from the connection server. If it is determined in step 804 that the inviting instant messaging user is currently logged in to the instant messaging system and, therefore, is available to participate in an instant messaging session with the requesting guest user, the process proceeds to step 808 in which the guest event server assigns a guest user identification to the guest user and associates the guest user identification with the guest user and the guest user's login data. In one embodiment, the guest user identification assigned to the guest user is valid only for instant messaging communication with the inviting instant messaging user, that is the registered instant messaging user associated with the HTML messenger toolbox initially invoked by the guest user. In one embodiment, the guest login server is configured to ensure that only

Nintendo Exhibit 1003
Part 1 of 2
Page 00553

three guest user identifications may be associated with any IP address at a given time, as a protection against the guest user feature being used inappropriately, such as to send large amounts of unwanted and unsolicited messages to one or more inviting instant messaging users.

In step 810 of the process shown in Figure 8, an instant messaging session is established by the connection server between the guest user and the inviting instant messaging user. In one embodiment, establishing the instant messaging session comprises associating the guest user identification with the inviting user's identification and assigning an instant messaging session identifier to the instant messaging session between the guest user and the inviting user. In one embodiment, this information is used by the guest login server to ensure that messages received from the guest user and the inviting user are processed correctly.

In step 812 of the process shown in Figure 8, the guest user identification assigned to the guest user is sent by the connection server to the browser-executable instant messaging client at the guest user instant messaging client at the guest user's client system. The log in process ends in step 814.

Figure 9 is a flowchart illustrating a process executed in one embodiment by the browser-executable client at the invited user's client system to send and receive instant messages between the invited user and the registered user associated with the HTML messenger toolbox when the invited user has logged in as a guest user. In step 902, the browser-executable client receives the guest user identification assigned and sent by the connection server. In step 904, the guest user identification assigned by the connection

Nintendo Exhibit 1003
Part 1 of 2
Page 00554

server is used to send the initial instant messaging message entered by the guest user in the HTML messenger toolbox, as described above to the inviting instant messaging user.

In step 906, an instant messaging user interface is displayed to the guest user.

In step 908, instant messages entered by the guest user in the message entry area of the instant messaging user interface displayed in step 906 are received and sent by the browser-executable client as instant messages addressed to the inviting instant messaging user associated with the HTML messenger toolbox. As shown in Figure 9, this is repeated whenever the guest user enters and submits a new message.

In step 910 of the process shown in Figure 9, the browser-executable client receives and displays to the guest user instant messages received from the inviting instant messaging user associated with the HTML messenger toolbox invoked by the guest user and/or messages received from the instant messaging connection server. As shown in Figure 9, the step 910 is repeated each time a new message is received.

In step 912, the browser-executable client receives and processes an indication that a participant in the instant messaging session has logged off. If the participant logging off is the guest user, the indication is received in one embodiment when the guest user selects a log off option in the instant messaging display. In one embodiment, the indication is received when the guest user selects an option to close the instant messaging window. If the participant logging off is the guest user, the browser-executable client sends an indication to the connection server that the guest user has logged off. If, on the other hand, the participant logging off is the inviting instant messaging user, the browser-executable client receives an indication that the inviting user has logged off in the form of a message received from the connection server. If the browser-executable client receives

Nintendo Exhibit 1003
Part 1 of 2
Page 00555

such an indication from the connection server that the inviting instant messaging user has logged off, the browser-executable client displays to the guest user a message indicating that the inviting instant messaging user has logged off. In one embodiment, the browser-executable client is configured to disable the sending of any further messages by the guest user once an indication has been received that the inviting user has logged off. In one alternative embodiment, the browser-executable client is not so configured and the guest message server is instead configured to disallow the sending of any further messages by the guest user once an indication has been received that the inviting user has logged off.

Figure 10 is an illustration of an exemplary guest user instant messaging user interface display 1000 provided to a guest user in one embodiment, as in step 906 of Figure 9. The display 1000 comprises a target recipient identification display area 1002 in which information identifying the inviting instant messaging user is displayed. In the example shown in Figure 10, the inviting instant messaging user is identified as "sender" to indicate the fictitious sender of an electronic mail message incorporating an HTML messenger toolbox such as the one shown in Figure 4. The display 1000 further comprises a guest user identification display area 1004 in which the guest user identification may be displayed. In one embodiment, the guest user identification assigned by the connection server is displayed. In one embodiment, the display name provided by the guest user is displayed. In one embodiment, both the guest user identification and the display name are displayed.

The display 1000 further comprises a message text display area 1006 in which messages sent by the various participants of the instant messaging session, and/or by the

Nintendo Exhibit 1003
Part 1 of 2
Page 00556

instant messaging system, are displayed. As shown in Figure 10, the first message displayed in the display area 1006 is the initial message entered by the guest user in the initial message entry area of the HTML messenger toolbox. Subsequent messages would be displayed in the order in which they are sent, each message being associated with its sender. The message display area 1006 comprises a scroll bar control 1008 which may be used in the well known manner to scroll up or down to see message text that is not currently displayed in the message display area 1006.

The display 1000 further comprises a message entry area 1010 in which the guest user may enter the text of the message the guest user wishes to send to the inviting instant messaging user. The display 1000 further comprises a "send" button 1012, which the guest user may select to submit the text entered in the message entry area 1010 for processing and transmission to the inviting instant messaging user.

The display 1000 further comprises an instant messaging display window control bar 1014, which control bar comprises a close window control button 1016. In one embodiment, selection of the close window control button 1016 provides an indication to the browser-executable client that the guest user is logging off, as described above, and causes the instant messaging display window to close.

Figure 11 is a flowchart illustrating a process used in one embodiment at the guest message server to process instant messages sent by a guest user. In step 1102, a message from the guest user to the inviting user is received at the connection server. In step 1104, the guest message server verifies that the message is addressed to the inviting instant messaging user for which the guest user identification is valid.

Nintendo Exhibit 1003
Part 1 of 2
Page 00557

In step 1106, if it has been determined that the message is not addressed to the inviting instant messaging user for which the guest user identification is valid, the process proceeds to step 1108, in which an error message is returned to the guest user. If it has been determined in step 1106 that the message is addressed to the inviting instant messaging user for which the guest user identification is valid, the process proceeds to step 1110 in which the guest message server confirms that the inviting instant messaging user is still on line. In step 1112, if it has been determined that the inviting instant messaging user is not on line, the process proceeds to step 1114, in which an error message is returned to the guest user indicating that the inviting instant messaging user is not on line. If it has been determined in step 1112 that the inviting instant messaging user is on line, the message is delivered to the inviting instant messaging user in step 1116. In one embodiment, in step 1116, the connection server places the message in a form suitable for being sent to the inviting instant messaging user. In one embodiment, the form in which the message is placed prior to being sent to the inviting instant messaging user is determined at least in part by the version of the client side instant messaging application software installed at the inviting user's client system.

Figure 12 is an illustration of an instant messaging display 1200 used in one environment to provide an instant messaging user interface to a registered instant messaging user for an instant messaging session with a guest user that is not a registered instant messaging user. The display 1200 comprises a target recipient identification display area 1202 in which an identification of the party to whom instant messages entered in the instant messaging window will be sent is displayed. In the example shown in Figure 12, the target recipient is identified as "guest user". In one embodiment, the

Nintendo Exhibit 1003
Part 1 of 2
Page 00558

identification displayed in display area 1202 would be the guest user identification assigned by the connection server to the guest user. In one embodiment, the identification displayed in display area 1202 would be a display name entered by the guest user upon log in as described above. The display 1200 further comprises an originator identification display area 1204 in which identification of the sender of instant messages by means of the instant messaging window is displayed. In the example shown in Figure 12, the originator is identified as "sender" to refer to the inviting user as the sender of the original electronic mail message containing the HTML messenger toolbox invoked by the guest user to engage in instant messaging with the sender.

The display 1200 further comprises a message text display area 1206 in which instant messages sent by any participant in the instant messaging session, or by the system, are displayed. In one embodiment, not illustrated in Figure 12, a legend is provided at the top of the message text display area 1206, prior to displaying the first message from the guest user, which legend advises the inviting instant messaging user that the party with whom the instant messaging session is being conducted is a guest user and not a registered user of the instant messaging system. In one embodiment, the legend comprises instructions as to limitations or other differences in the functionality of the instant messaging system or program that may result from the fact that the other participant in the instant messaging session is not a registered user. For example, in one embodiment, the registered instant messaging user is warned that the guest user may not be the person he or she purports to be.

The display 1200 further comprises an instant message entry area 1208 in which the registered instant messaging user may enter instant messages to be sent to the guest

Nintendo Exhibit 1003
Part 1 of 2
Page 00559

user. The display 1200 further comprises a "send" button 1210, which the registered instant messaging user may select to send an instant message entered in the instant message entry area 1208 to the connection server for processing and delivery to the guest user.

The display 1200 further comprises a tool bar 1212 comprising a plurality of icons 1214, each of which corresponds to a function, operation, or service provided by the client side instant messaging application software. In one embodiment, when the other participant in the instant messaging session is a guest user, the display 1200 is modified such that only those functions that are available to the registered user for use with respect to an instant messaging session with a guest user are displayed in the tool bar 1212. In one embodiment, all of the icons normally included in the tool bar 1212 are displayed when the other participant is a guest user, but certain functions may be disabled by operation of the client side instant messaging application software when the other participant is a guest user. In one embodiment, the user identification of a participant in an instant messaging session may normally be added to a list of "friends" with whom the registered user more regularly communicates, and in one such embodiment this feature is disabled with respect to a guest user such that the guest user identification may not be added to the registered user's list of "friends". In one embodiment, features are disabled with respect to a guest user if the browser-executable instant messaging client being used by the guest user cannot support the feature, such as a feature providing advanced functionality such as voice communication. In one embodiment, if a registered user attempts to initiate an operation that is not valid with respect to a guest user, the client

Nintendo Exhibit 1003
Part 1 of 2
Page 00560

side application software returns an error message informing the user that the operation is not valid with respect to a guest user.

The display 1200 further comprises a browser window control bar 1216, which control bar comprises a window close control button 1218. In one embodiment, selection of the window close control button 1218 causes the client side instant messaging application software to send an indication to the connection server that the inviting instant messaging user has disconnected. In one alternative embodiment, closing the instant messaging window does not cause an indication to be sent to the connection server that the inviting instant messaging user has disconnected, and a registered user must instead select a separate option to disconnect or exit completely from the client side instant messaging software in order for such an indication to be sent. In one embodiment, a disconnect control button, not shown in Figure 12, is included in the display 1200 to enable the registered user to indicate a desire to disconnect.

In one embodiment, the display 1200 further comprises a button which, when selected by the inviting instant messaging user, sends to the guest user a preformatted message inviting the guest user to become a registered user of the instant messaging system and thereby make it possible for the registered user and the guest user to communicate in an instant messaging session in which all of the features of the instant messaging system are available to both parties.

Figure 13 is a flowchart illustrating a process used in one embodiment to process at the connection server instant messages sent from a registered instant messaging user to a guest user. In step 1302, an instant message from the registered instant messaging user to the guest user is received at the connection server. In step 1304, the connection server

Nintendo Exhibit 1003
Part 1 of 2
Page 00561

verifies that the registered user who sent the message is a user authorized to send a message to the guest user. In one embodiment, only the inviting user, i.e., the registered user associated with the HTML messenger toolbox invoked by the guest user, may send instant messages to the guest user. In step 1306, if it is determined that the sender of the messages is not authorized to send messages to the guest user, the process proceeds to step 1308 and an error message is returned to the sender of the message informing the sender that the sender is not authorized to send messages to the guest user. If it is determined in step 1306 that the sender of the messages is authorized to send messages to the guest user, the process proceeds to step 1310 in which the connection server confirms that the guest user is still connected to the instant messaging system. In step 1312, if it is determined that the guest user has logged off, the process proceeds to step 1314 in which an error message is returned to the registered user informing the registered user that the guest user has logged off. If it is determined in step 1312 that the guest user is still on line, the process proceeds to step 1316 in which the instant message is delivered to the guest user. In one embodiment, the messages are delivered to the guest user in a streamlined format that omits information identifying the sender of the message, because the browser-executable client at the guest user's client system is configured to assume that messages delivered from the connection server to the guest user originated from the registered instant messaging user authorized to send messages to the guest user.

Figure 14 is a flowchart illustrating a process used in one embodiment to process, at the connection server an indication that either the guest user or the inviting user has logged off, as in step 208 of the process shown in Figure 2. With respect to a guest user, the process begins with step 1402 in which an indication is received at the connection

Nintendo Exhibit 1003
Part 1 of 2
Page 00562

server that the guest user has logged off. As described above, in one embodiment the browser-executable client at the guest user's client system sends such an indication to the connection server when the guest user indicates a desire to log off. In step 1404, the connection server informs the inviting instant messaging user that the guest user has logged off. In one embodiment, the client side instant messaging software installed at the inviting user's client system displays a message to the user upon receipt of the indication from the connection server and disables any further messages being sent to the guest user from the client system.

With respect to an indication received from the inviting instant messaging user, the process shown in Figure 14 begins with step 1406, in which an indication is received at the connection server that the inviting instant messaging user has logged off. In step 1408, the connection server sends a message to the guest user informing the guest user that the inviting user has logged off. In one embodiment, the browser-executable client at the guest user's client system responds to receipt of an indication from the connection server that the inviting user has logged off by displaying a message to the guest user and by disabling any further messages being sent by the guest user.

Once the connection server has either sent a message to the inviting user in step 1404 or to the guest user in step 1408 as appropriate, the process shown in Figure 14 proceeds to step 1410 in which the connection server terminates the instant messaging session between the inviting user and the guest user. In one embodiment, the termination of the instant messaging session in step 1410 comprises disabling the sending of any further messages between the inviting user and the guest user. In one embodiment, the termination of the instant messaging session in step 1410 comprises deleting one or more

Nintendo Exhibit 1003
Part 1 of 2
Page 00563

records so that the inviting user and the guest user are no longer associated with a valid instant messaging session identifier.

In step 1412, the guest user is disconnected from the instant messaging system. In one embodiment, the guest user is disconnected by rendering invalid the temporary guest user identification assigned to the guest user.

In step 1414, the guest user identification assigned to the guest user is discarded and deleted from any lists of currently valid user identifications maintained by the connection server. In one embodiment, the guest user identification is discarded by the system as part of the process of disconnecting the guest user in step 1412 and, in such an embodiment, step 1414 is omitted. In step 1416, the use of the discarded guest user identification is disabled for a prescribed period of time. In one embodiment, the use of the guest user identification is disabled for a prescribed period of time to prevent the fraudulent and/or erroneous use of the guest user identification by any participant in the prior authorized instant messaging session in which the guest user identification was used.

While the examples described in detail above deal primarily with providing instant messaging functionality in an electronic mail environment, the approach described above may similarly be used in other context, such as web-based message groups, personal or other home pages, auction web sites, public calendars, or in any other web page or network accessible location associated with an instant messaging user, or with any HTML-based or HTML-compatible electronic message or other document sent by a registered instant messaging user in an any network environment. Also, while the examples described in detail above discuss the use of HTML and DHTML to provide

Nintendo Exhibit 1003
Part 1 of 2
Page 00564

certain functionality, other programming languages may also be used to provide the functionality described without requiring the user to complete an extensive download, installation, and registration process. Examples of such other languages and tools include, without limitation, clients comprising computer code written in Java, JavaScript, Flash, and/or Active X.

While certain of the embodiments described in detail above involve an instant messaging session between a single registered user and a single guest user, the instant messaging session may as well involve a plurality of guest users and/or a plurality of registered instant messaging users.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. It should be noted that there are many alternative ways of implementing both the process and apparatus of the present invention. Accordingly, the present embodiments are to be considered as illustrative and not restrictive, and the invention is not to be limited to the details given herein, but may be modified within the scope and equivalents of the appended claims.

WHAT IS CLAIMED IS:

Nintendo Exhibit 1003
Part 1 of 2
Page 00565

CLAIMS

1. A method for enabling a guest user who is not a registered user of an instant messaging system to communicate by instant messaging with a registered user of the system, the method comprising:

receiving an indication that the guest user desires to communicate with the registered user by instant messaging;

sending to a client computer system associated with the guest user browser-executable computer code comprising computer instructions for providing at least limited instant messaging functionality to the guest user at the client computer system, without requiring the guest user to download and install client side instant messaging application software and without requiring the guest user to register as a user of the instant messaging system; and

facilitating an instant messaging session between the guest user and the registered user.

2. The method of claim 1, wherein facilitating the instant messaging session comprises delivering instant messages from the guest user to the registered user.

3. The method of claim 1, further comprising providing an entry point configured to receive an indication from the guest user that the guest user desires to communicate with the registered user by instant messaging.

4. The method of claim 3, wherein the entry point is provided in an electronic mail message sent by the registered user to the guest user.

5. The method of claim 3, wherein the entry point is provided in a web page associated with the registered user.

Nintendo Exhibit 1003
Part 1 of 2
Page 00566

6. The method of claim 3, wherein the entry point is provided in an electronic document associated with the registered user.

7. The method of claim 3, wherein the entry point is provided by computer code comprising code written in the HyperText Markup Language (HTML).

8. The method of claim 1, further comprising receiving an indication from the registered user that the registered user would like to incorporate into an electronic mail message to the guest user an entry point configured to receive an indication from the guest user that the guest user desires to communicate with the registered user by instant messaging.

9. The method of claim 1, further comprising receiving an indication from the registered user that the inviting user would like to incorporate into a web page associated with the registered user an entry point configured to receive an indication from the guest user that the guest user desires to communicate with the inviting user by instant messaging.

10. The method of claim 1, wherein the computer code comprises a browser-executable instant messaging client

11. The method of claim 10, wherein the browser-executable instant messaging client comprises computer instructions in the Dynamic HyperText Markup Language (DHTML).

12. The method of claim 10, wherein the browser-executable instant messaging client comprises computer instructions in JavaScript.

Nintendo Exhibit 1003
Part 1 of 2
Page 00567

13. The method of claim 10, wherein the browser-executable instant messaging client comprises computer instructions in ActiveX.

14. The method of claim1, further comprising assigning a temporary user identification to the guest user.

15. The method of claim 14, wherein the temporary user identification is unique to the guest user during the period during which it is assigned to the guest user.

16. The method of claim 14, wherein the temporary user identification is at least temporarily deactivated upon termination of the instant messaging session between the guest user and the registered user.

17. The method of claim 14, wherein the temporary user identification is valid only for instant messaging with the registered user.

18. The method of claim 14, wherein the number of temporary user identifications that may be assigned at any given time to the IP address associated with the client computer system is limited.

19. The method of claim 1, further comprising prompting the guest user to provide a display name by which the guest user may be identified to the registered user.

20. The method of claim 1, wherein the instant messaging system is associated with at least one other registration-based service in which some users may be registered with the other service but not the instant messaging system and in which the users of the other service sign in using a user name to access the other service, the method further comprising:

determining if the guest user is signed in as a user of the other service; and

Nintendo Exhibit 1003
Part 1 of 2
Page 00568

if the user is signed in as a user of the other service, using the user name associated with the guest user with respect to the other service as a display name to identify the guest user to the registered user.

21. The method of claim 20, wherein cookie information is used to determine if the guest user is signed in as a user of the other service.

22. The method of claim 1, wherein the computer code is configured to display an instant messaging window to the guest user.

23. The method of claim 22, wherein the instant messaging window comprises an area for displaying messages sent by either the guest user or the registered user.

24. The method of claim 22, wherein the instant messaging window comprises an area for entering the text of a message to be sent and displayed to the registered user essentially in real time.

25. The method of claim 1, further comprising advising the registered user that the guest user is not a registered user.

26. The method of claim 1, wherein the registered user is associated with a registered user client computer system on which client side instant messaging application software associated with the instant messaging system is installed and the method further comprises disabling, at least with respect to the guest user, at least one feature of the client side instant messaging application software installed on said registered user client computer system.

27. The method of claim 26, wherein the disabled feature is one that would otherwise have allowed the registered user to add the temporary user identification assigned to the

Nintendo Exhibit 1003
Part 1 of 2
Page 00569

guest user to a list of users whose online presence is monitored by the client side instant messaging application software installed on said second client computer system.

28. The method of claim 26, wherein the disable feature is one that the computer code sent to the guest user's client computer system does not support.

29. A method for enabling an invited user who may not be a registered user of an instant messaging system having client side instant message application software associated with it to communicate by instant messaging with an inviting user who is a registered user of the system, the method comprising:

receiving an indication that the invited user desires to communicate with the inviting user by instant messaging;

sending to a client computer system associated with the invited user browser-executable computer code comprising computer instructions for:

determining whether the client side instant messaging application software associated with the instant messaging system is installed in the client computer system; and

in the event it is determined that the client side instant messaging application software associated with the instant messaging system is not installed in the client computer system, providing at least limited instant messaging functionality to the invited user at the client computer system, without requiring the invited user to download and install the client side instant messaging application software and without requiring the invited user to register as a user of the instant messaging system; and

Nintendo Exhibit 1003
Part 1 of 2
Page 00570

facilitating an instant messaging session between the invited user and the inviting user.

30. The method of claim 29, further comprising:

in the event it is determined that the client side instant messaging application software associated with the instant messaging system is installed in the client computer system, activating and using the installed client side instant messaging application software to enable the invited user to communicate with the inviting user by instant messaging.

31. The method of claim 29, wherein said computer instructions for determining whether the client side instant messaging application software associated with the instant messaging system is installed in the client computer system comprises computer code written in the JavaScript programming language.

32. The method of claim 29, wherein said computer instructions for determining whether the client side instant messaging application software associated with the instant messaging system is installed in the client computer system comprises computer code written in the VBScript programming language.

33. The method of claim 29, wherein said computer instructions for determining whether the client side instant messaging application software associated with the instant messaging system is installed in the client computer system comprises computer code written in the ActiveX programming language.

34. A system for enabling a guest user who is not a registered user of an instant messaging system to communicate by instant messaging with a registered user of the system, comprising:

Nintendo Exhibit 1003
Part 1 of 2
Page 00571

a web server configured to:

receive an indication that the guest user desires to communicate with the registered user by instant messaging; and

send to a client computer system associated with the guest user browser-executable computer code comprising computer instructions for providing at least limited instant messaging functionality to the guest user at the client computer system, without requiring the guest user to download and install client side instant messaging application software and without requiring the guest user to register as a user of the instant messaging system; and

an instant messaging server configured to facilitate an instant messaging session between the guest user and the registered user.

35. The system of claim 34, wherein said web server comprises a plurality of servers.

36. The system of claim 34, wherein said instant messaging server comprises as plurality of servers.

37. A computer program product embodied on a computer readable medium for enabling a guest user who is not a registered user of an instant messaging system to communicate by instant messaging with a registered user of the system, the computer program product comprising computer instructions for:

receiving an indication that the guest user desires to communicate with the registered user by instant messaging;

Nintendo Exhibit 1003
Part 1 of 2
Page 00572

sending to a client computer system associated with the guest user browser-executable computer code comprising computer instructions for providing at least limited instant messaging functionality to the guest user at the client computer system, without requiring the guest user to download and install client side instant messaging application software and without requiring the guest user to register as a user of the instant messaging system; and

facilitating an instant messaging session between the guest user and the registered user.

Nintendo Exhibit 1003
Part 1 of 2
Page 00573

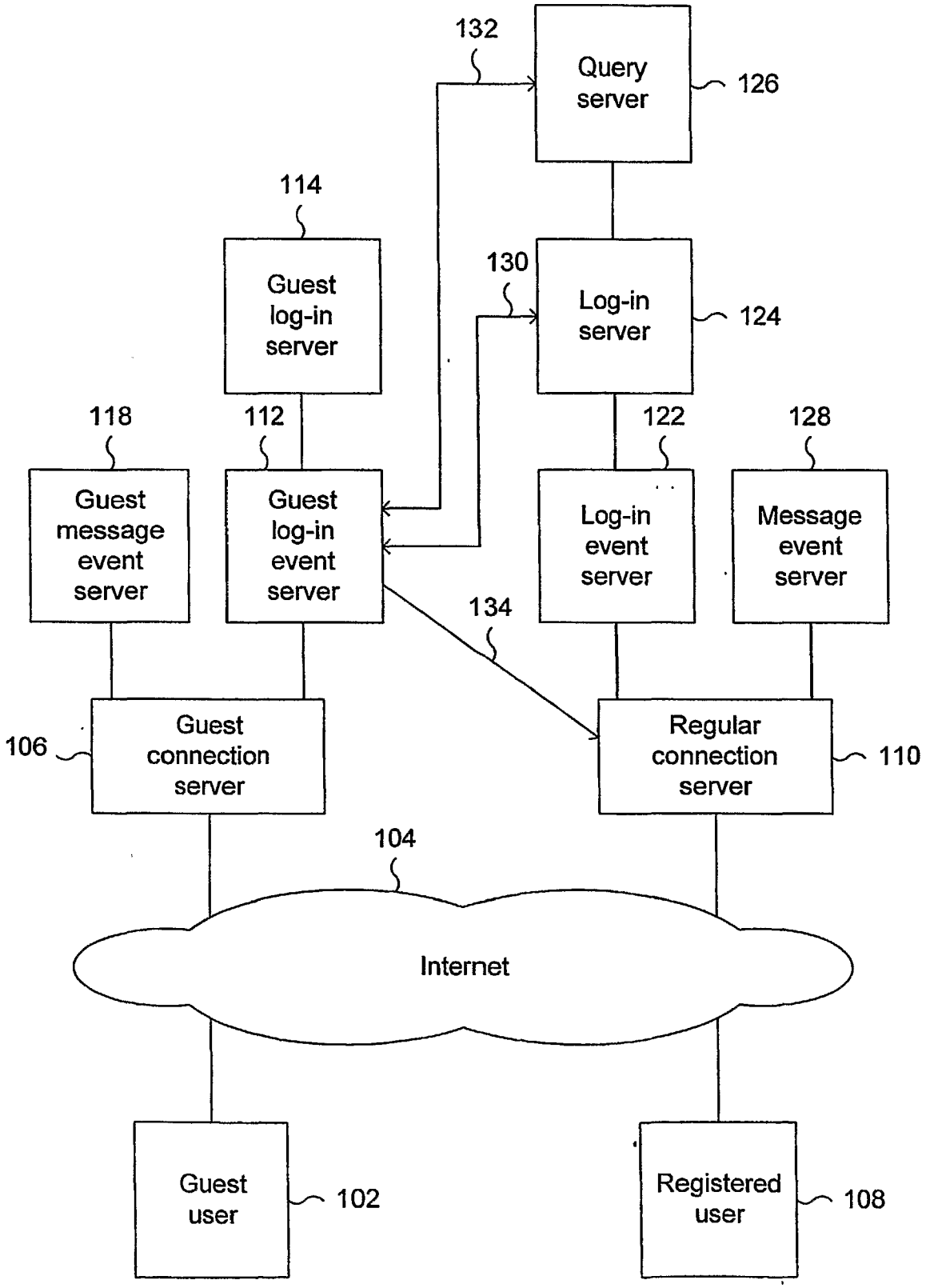


Figure 1A

SUBSTITUTE SHEET (RULE 26)

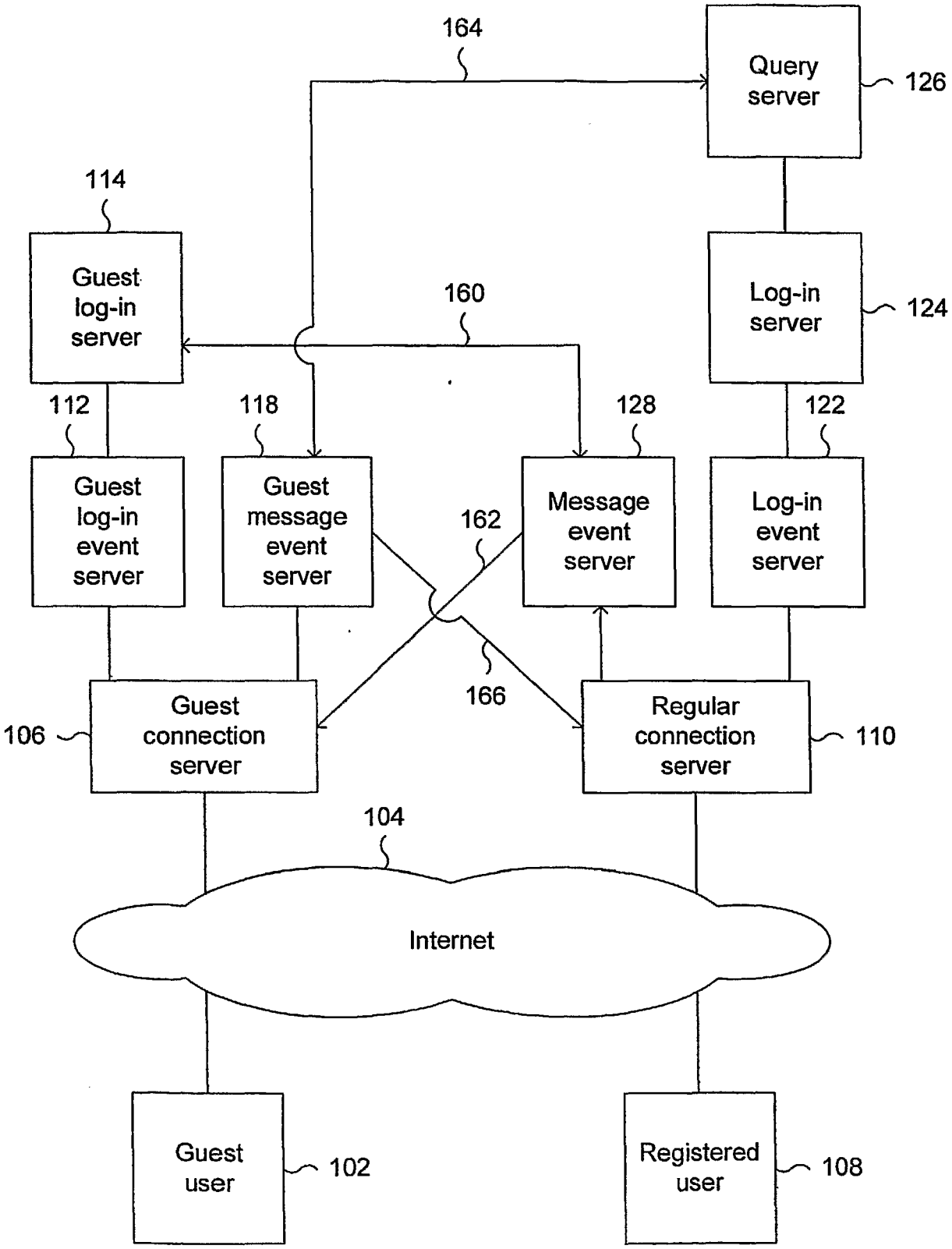


Figure 1B

Nintendo Exhibit 1003
Part 1 of 2
Page 00575

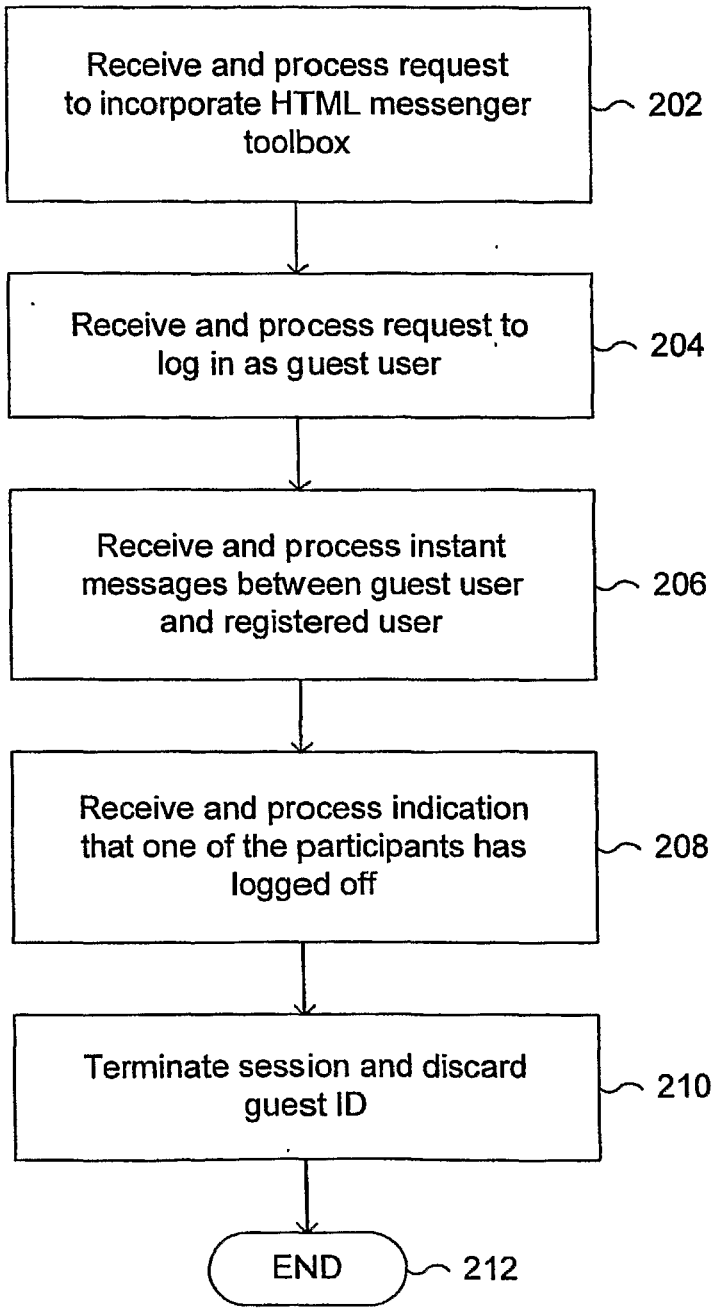

Receive and process request to incorporate HTML messenger toolbox
202
Receive and process request to log in as guest user
204
Receive and process instant messages between guest user and registered user
206
Receive and process indication that one of the participants has logged off
208
Terminate session and discard guest ID
210
END
212

Figure 2

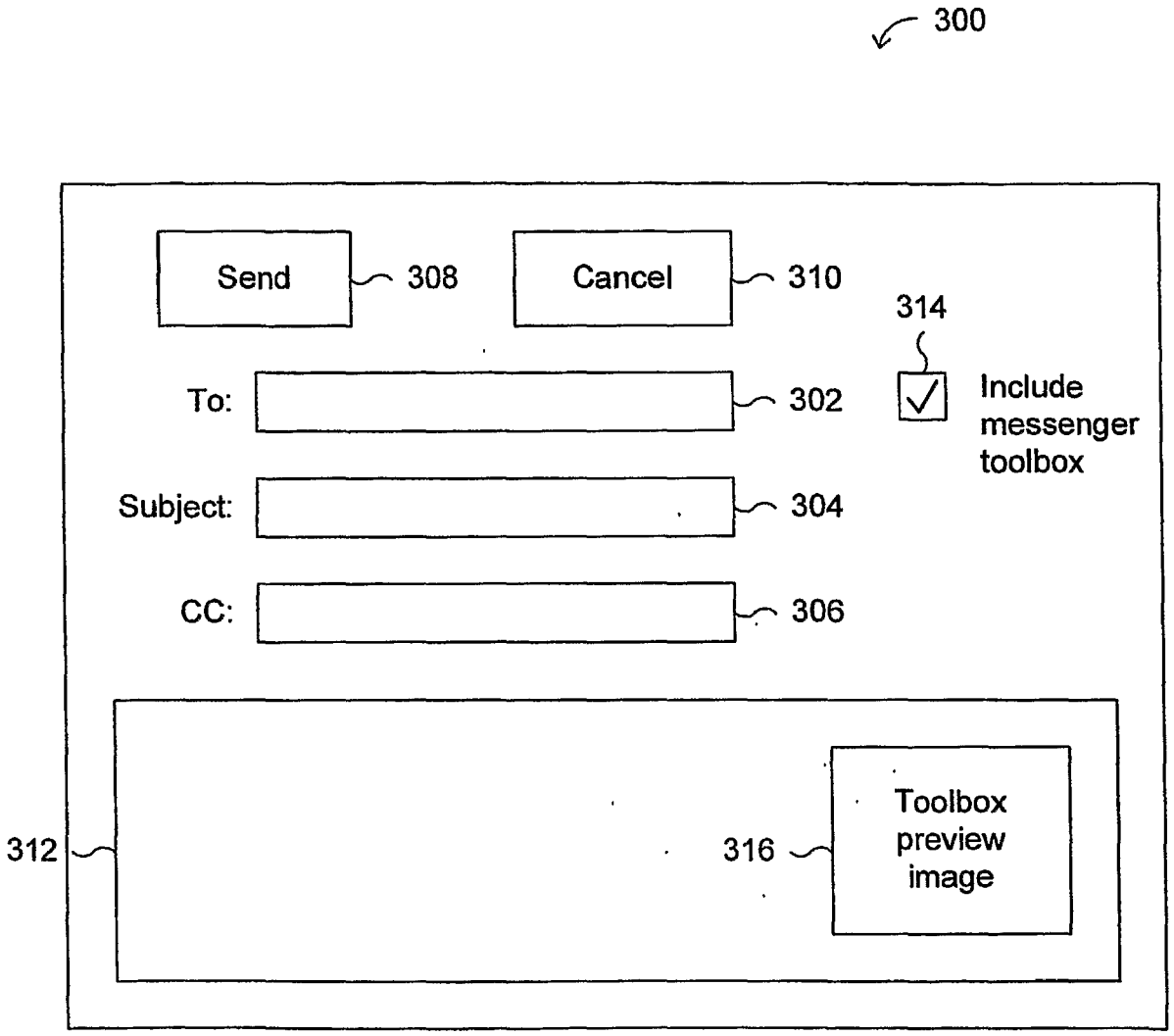


Figure 3

SUBSTITUTE SHEET (RULE 26)

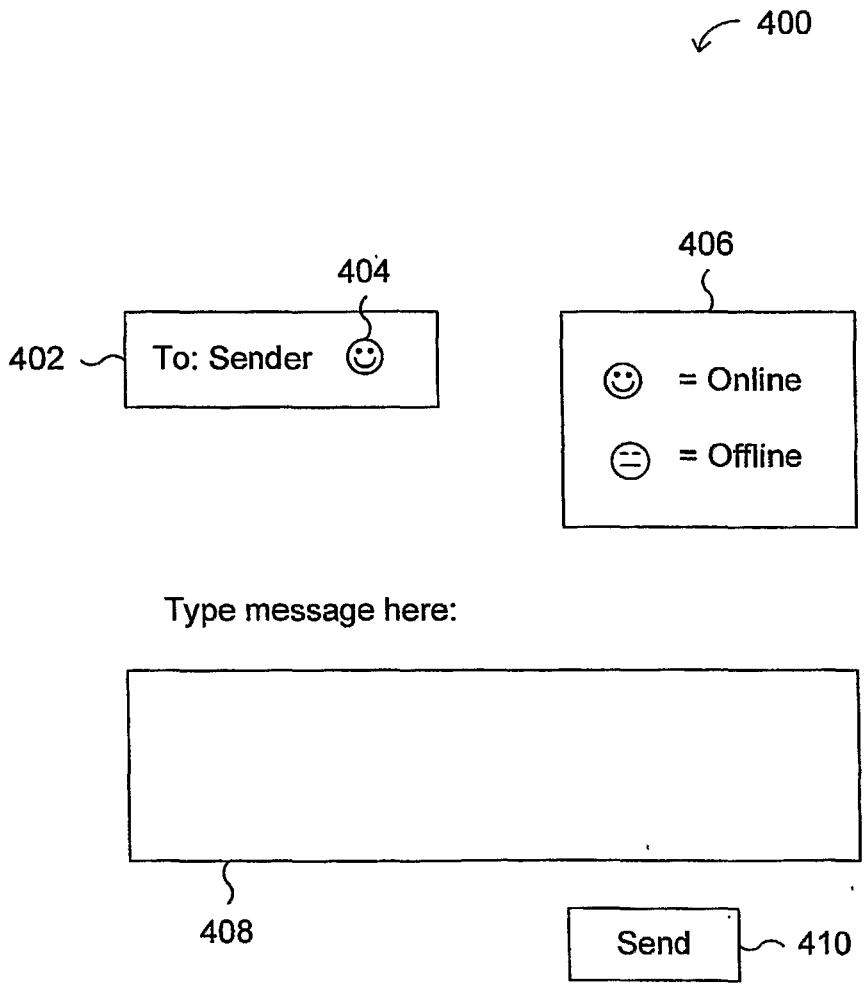


Figure 4

SUBSTITUTE SHEET (RULE 26)

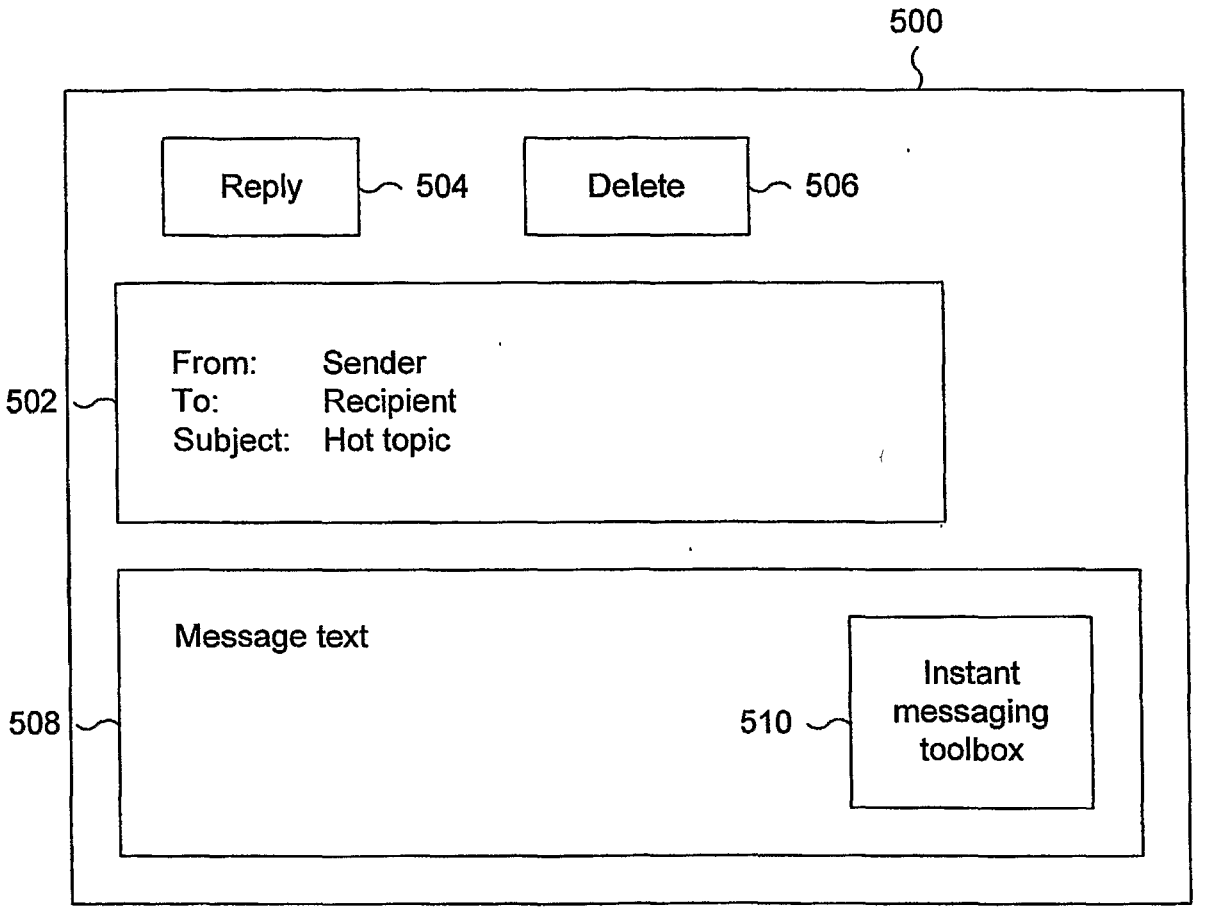


Figure 5

SUBSTITUTE SHEET (RULE 26)

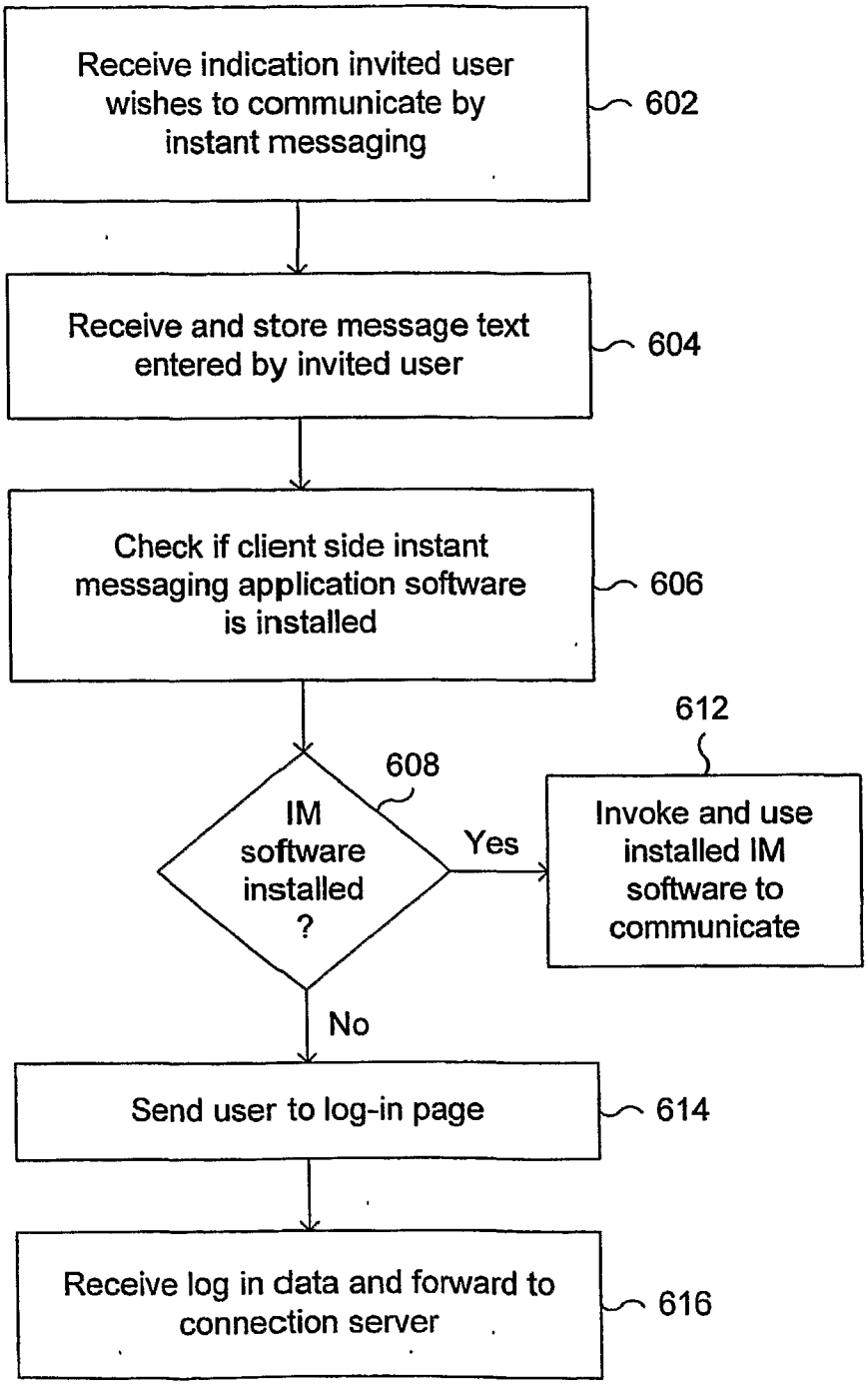


Figure 6

SUBSTITUTE SHEET (RULE 26)

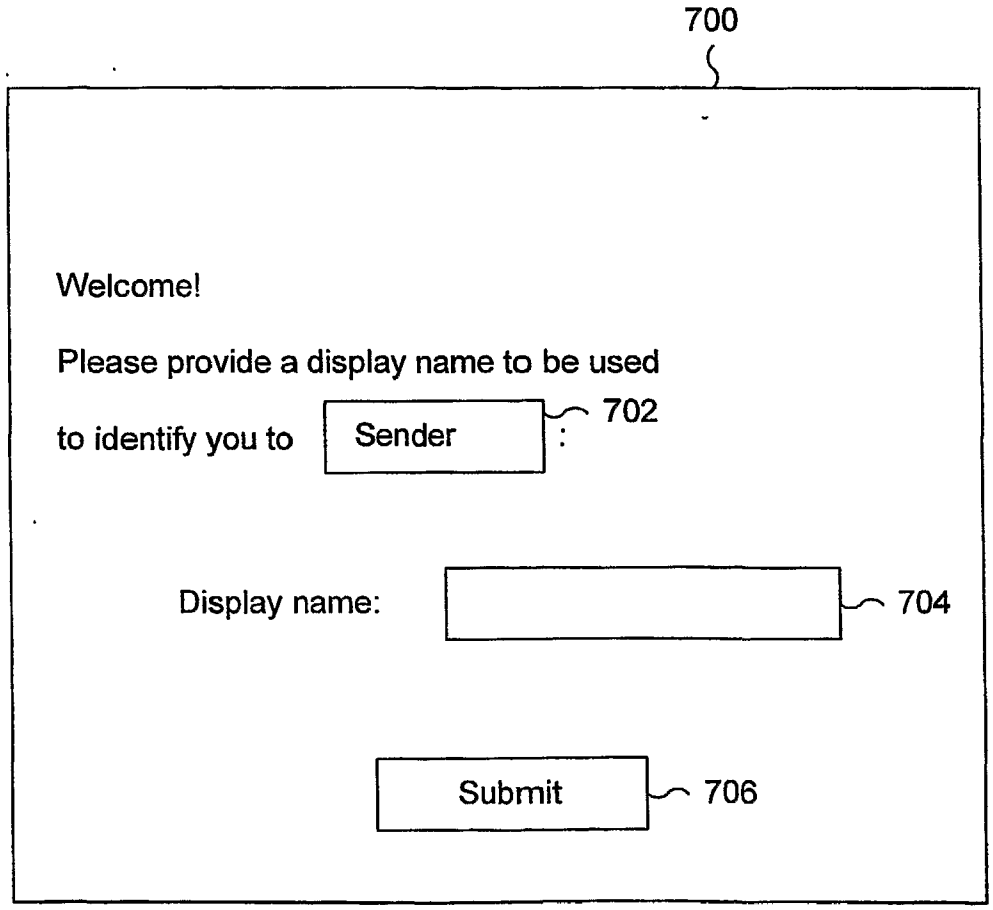


Figure 7

SUBSTITUTE SHEET (RULE 26)

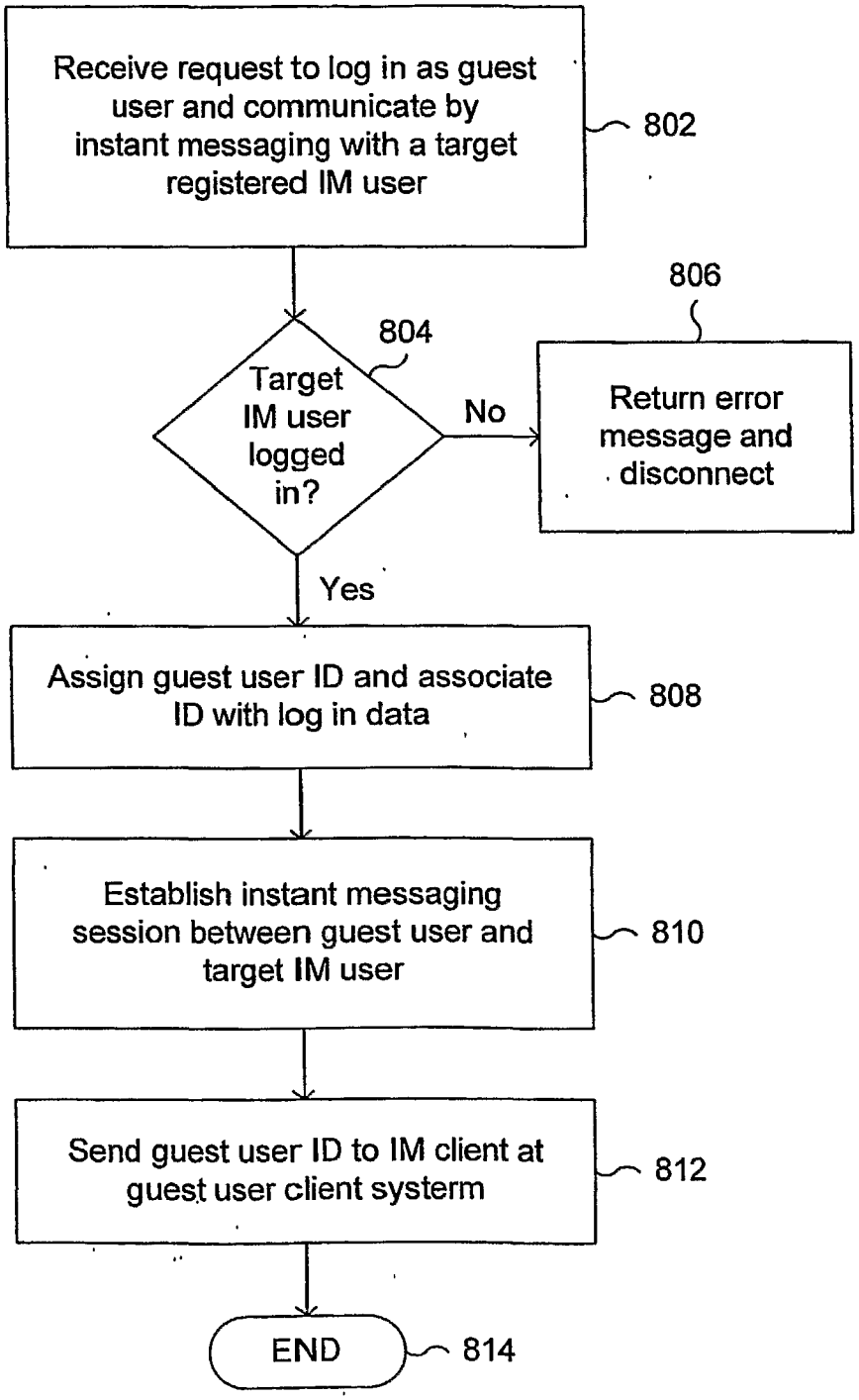


Figure 8

SUBSTITUTE SHEET (RULE 26)

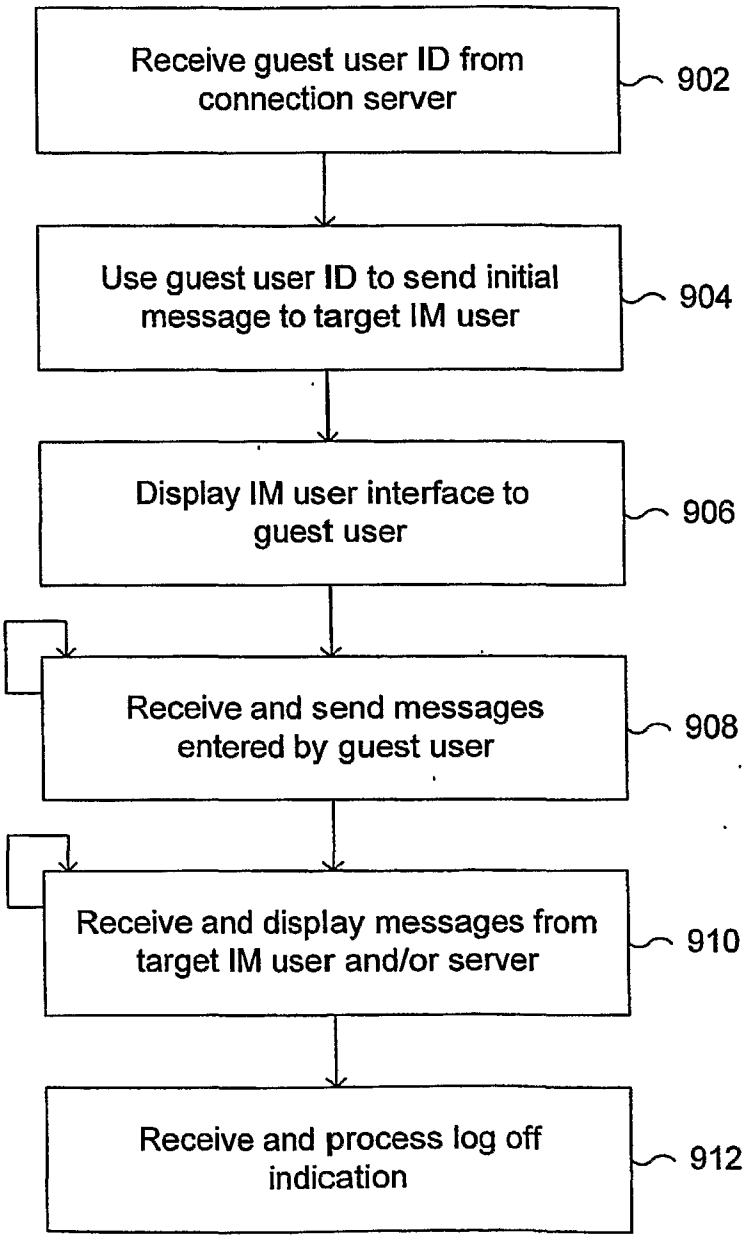


Figure 9

SUBSTITUTE SHEET (RULE 26)

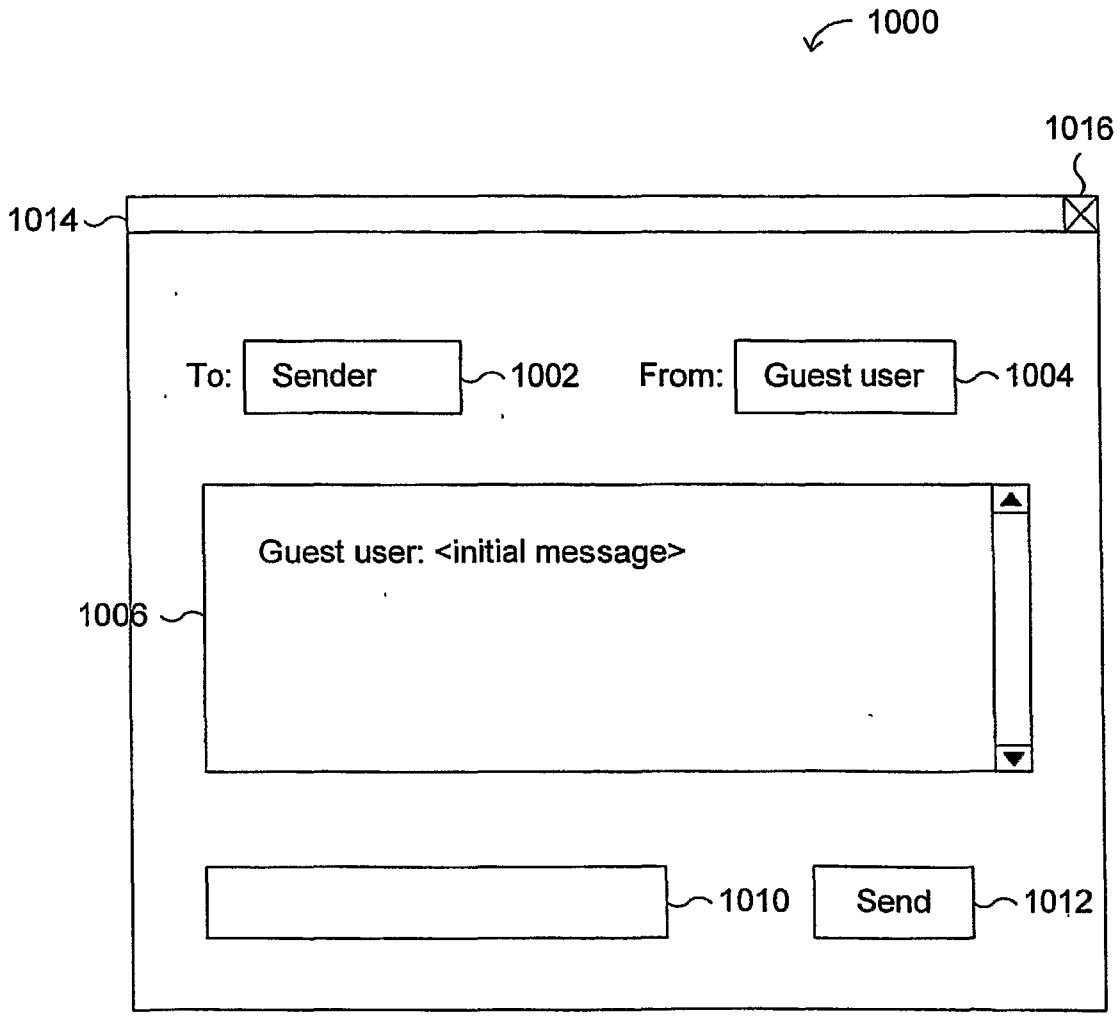


Figure 10

SUBSTITUTE SHEET (RULE 26)

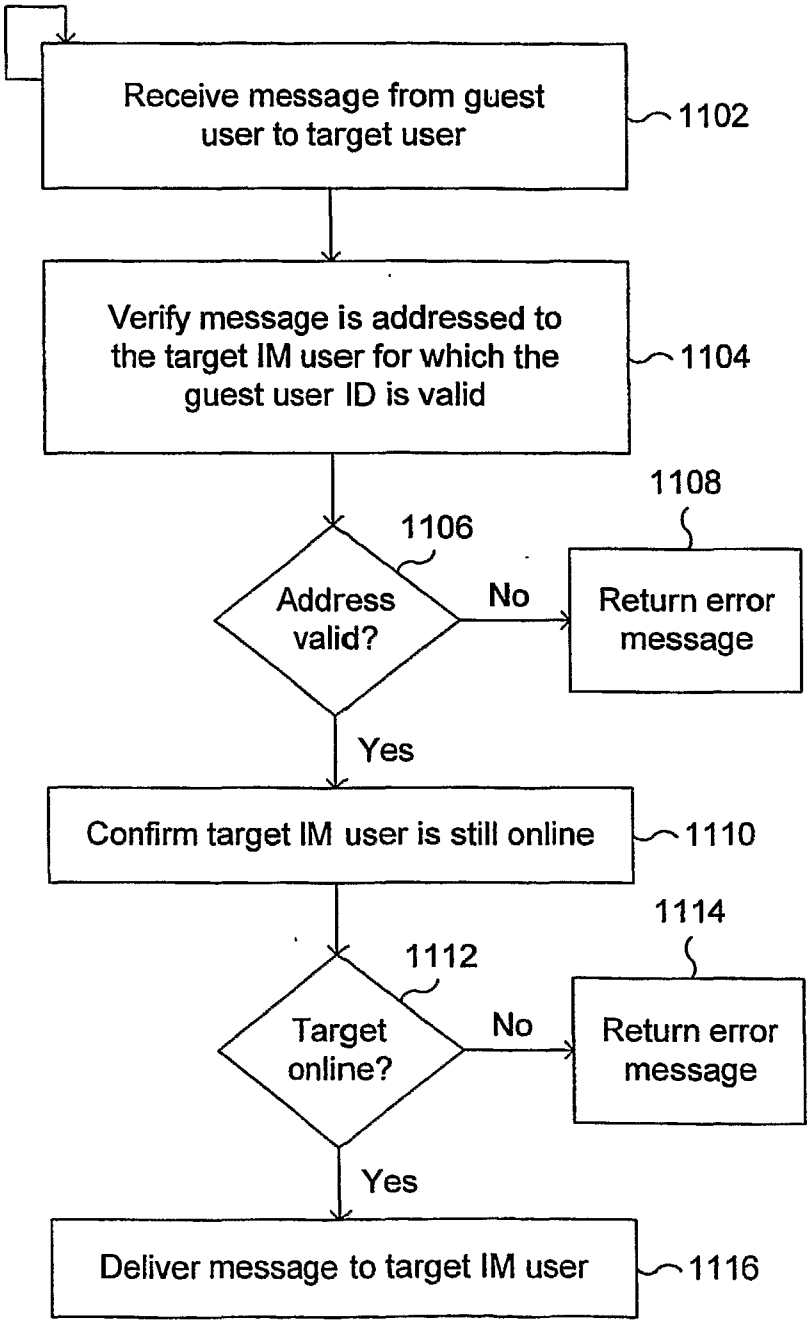


Figure 11

SUBSTITUTE SHEET (RULE 26)

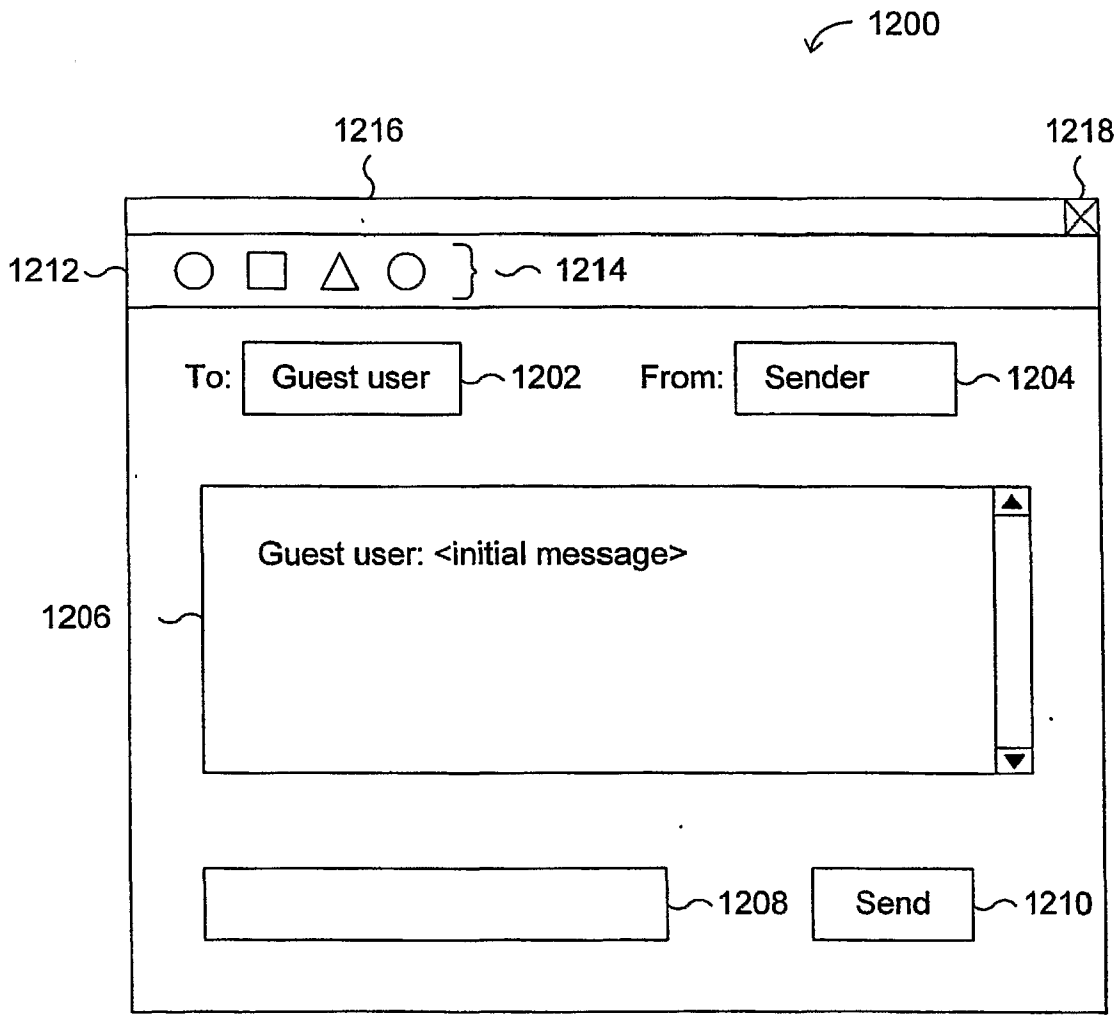

1200
1216
1218
1212
1214
To:
Guest user
1202
From:
Sender
1204
Guest user: <initial message>
1206
1208
Send
1210

Figure 12

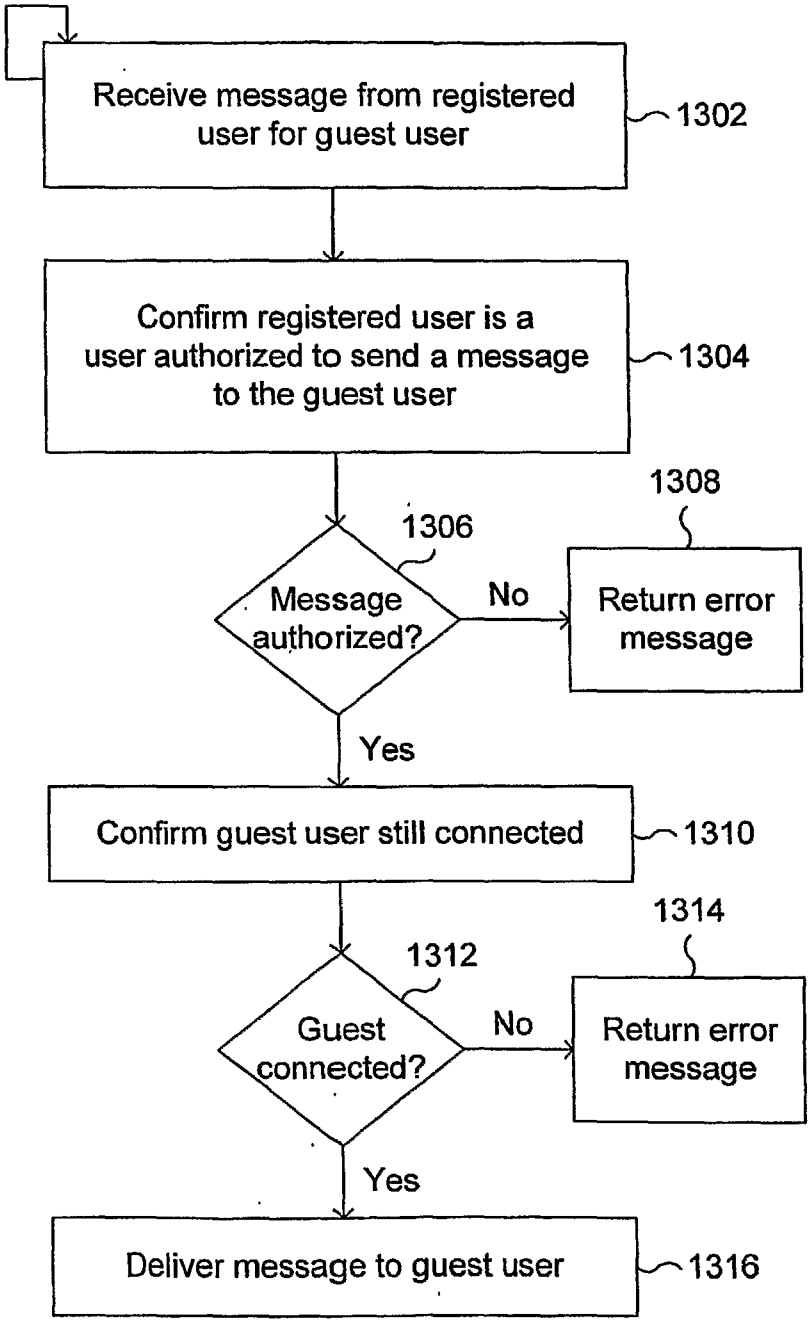


Figure 13

SUBSTITUTE SHEET (RULE 26)

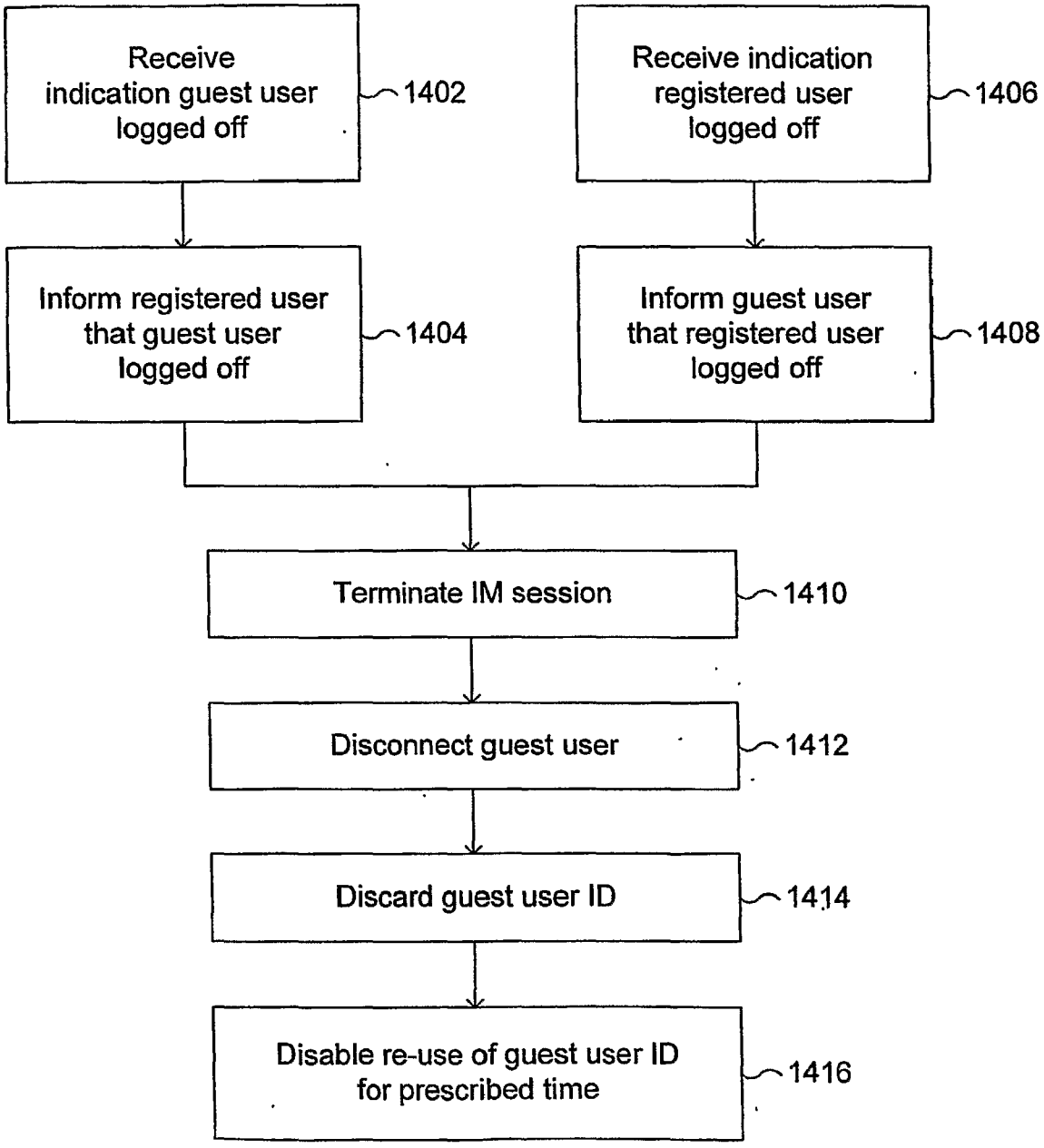

Receive indication guest user logged off
1402
Receive indication registered user logged off
1406
Inform registered user that guest user logged off
1404
Inform guest user that registered user logged off
1408
Terminate IM session
1410
Disconnect guest user
1412
Discard guest user ID
1414
Disable re-use of guest user ID for prescribed time
1416

Figure 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/01572

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04Q 7/20; H04L 9/32
US CL : 709/206; 713/201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/206

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PALM, EAST, ACM, IEEE, Google

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DigiChat Product Information. http://www.digichat.com/PI_featureSet.html Entire Document, especially page 1.	1-37
A,P	FIELD, A. Instant Messaging Comes of Age for Enterprise. Newsfactor Network, pages 1-4, especially pages 1-2.	1-37
Y	US 2001/0003202 A1 (MACHE et al) 7 June 2001 (07.06.2001), [0143].	1-37
Y,P	US 2002/0152402 A1 (TOV et al) 17 October 2002 (17.10.2002), [0010-0012], [0020-0025], [0030-0059].	1-37
Y	US 2002/0006803 A1 (MENDIOLA et al), 17 January 2002 (17.01.2002), Abstract, [0019-0035].	1-37

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
27 March 2003 (27.03.2003)

Date of mailing of the international search report
07 MAY 2003

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
David A Wiley
Peggy Harrod
Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 185 923 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
31.03.2004 Bulletin 2004/14

(21) Application number: **00920917.2**

(22) Date of filing: **20.04.2000**

(51) Int Cl.[7]: **G06F 9/00**

(86) International application number:
PCT/GB2000/001557

(87) International publication number:
WO 2000/067112 (09.11.2000 Gazette 2000/45)

(54) **A SYSTEM AND METHOD FOR MANAGING DISTRIBUTION OF CONTENT TO A DEVICE**

VORRICHTUNG UND VERFAHREN ZUM VERWALTEN DER VERTEILUNG VON INHALTEN ZU EINEM GERÄT

SYSTEME ET PROCEDE PERMETTANT DE GERER LA DISTRIBUTION D'UN CONTENU A UN DISPOSITIF

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GR IE IT LI LU MC NL PT SE

(30) Priority: **30.04.1999 GB 9910164**
21.09.1999 GB 9922348
06.10.1999 GB 9923640

(43) Date of publication of application:
13.03.2002 Bulletin 2002/11

(73) Proprietor: **elata Limited**
Poole, Dorset BH15 1EA (GB)

(72) Inventors:
- **JACKSON, Bruce**
  Poole, Dorset, BH12 5HT (GB)
- **BROOKES, Nigel Robert**
  Salisbury, Wiltshire SP1 2BA (GB)

(74) Representative: **Horner, David Richard et al**
D Young & Co,
21 New Fetter Lane
London EC4A 1DA (GB)

(56) References cited:
EP-A- 0 793 170
US-A- 5 581 764
US-A- 5 845 077
WO-A-91/08542
US-A- 5 797 128
US-A- 5 875 327

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 185 923 B1

Description

Field of the Invention

[0001] The present invention relates to a system and method for managing distribution of content to a device.

Description of the Prior Art

[0002] Content to be provided to a device may take a variety of different forms. For example, data files may be provided to the device for use with particular applications installed upon the device. Further, particular application programs may be distributed to the device for installation on the device in order to facilitate new functions, for example word processing programs, spreadsheet programs, e-mail programs, etc.

[0003] Up until now, much of the development of techniques for managing the distribution of content to devices has centered on the area of fixed computer devices connected to a computer network. Within such an environment, it is then possible to provide a localised management support structure to provide content on the network, and to control individual devices' access to that content.

[0004] For example, US-A-5,692,129 describes a technique for managing application programs in a computer network. When a computer networks is provided within an organisation, it is commonplace for a directory services database to be provided on the computer network to provide a "White Pages" style directory concerning people and other resources within the organisation. Often such directory service databases are object oriented databases. In accordance with the teaching of US-A-5,692,129, such an object oriented database is adapted to support the inclusion- of application -objects defining software applications available on the network. Further, certain types of objects in the database, such as user objects, are adapted to allow desktop attributes to be specified. An application object can then be added as a desktop attribute for such an object, to indicate that the corresponding application should be made available to the user represented by the object.

[0005] Additionally, US-A-5,692,129 specifies the use of a launcher application, which for a particular user can be arranged to retrieve that user's object, and to adapt the user's desktop to provide icons for any application specified by application objects identified in the user object's desktop attributes. Hence, by the above approach, a user's desktop can be automatically updated to indicate those applications that are installed on the network and are available to that user for accessing. The applications themselves are retained centrally on the network, and the user accesses them over the network.

[0006] US-A-5,581,764 describes a technique for managing the distribution of content to a device. In accordance with the technique of DI, a hierarchical structure of content is developed for a group of devices, this being referred to as a Schema in D1. Within the Schema, one or more dynamic linkages are provided, which when generating a "should have" (SH) list for any particular device, are resolved to determine which content should be provided to that device. To enable the resolution of the dynamic linkages, an initial interrogation process is required to determine the values of certain variables of the device.

[0007] Whilst this technique is clearly beneficial to computer devices that are permanently connected to the network, and hence able to run applications on the network, it is clearly not suitable for distributed devices that may only make periodic connections to a network, and when not connected to a network will still need to be self-contained (i.e. will need the content to be stored locally for their own use). However, such a scenario is becoming more and more commonplace, with the proliferation in portable computer devices, mobile phones, personal digital assistant devices (PDA), electronic organisers, etc. Whilst it is clearly desirable for an organisation to allow individuals within the organisation to use such portable devices, it makes it significantly more difficult to control and manage the distribution of content to those devices.

Summary of the Invention

[0008] Viewed from a first aspect, the present invention provides a system for managing distribution of content to a device, comprising: a database for storing a number of elements as a hierarchical structure of devices, content identifiers being able to be associated with elements in the hierarchical structure, and one of the elements representing the device; a server for referencing the hierarchical structure in the database to generate a profile for the device, the profile containing a number of content identifiers indicating content to be provided to the device, the profile containing any content identifiers associated with the element representing the device, along with any content identifiers associated with elements in the hierarchical structure from which that element depends; a device manager associated with the device and arranged to receive the profile from the server and to use the content identifiers in the profile to cause the content indicated by the profile to be provided to the device, a record being kept identifying the content provided to the device in accordance with the profile; the device manager further being arranged upon receipt of a subsequent profile from the server to compare the content identifiers in the subsequent profile with the record to determine new content not yet provided on the device and old content no longer to be provided on the device, the device manager being arranged to use the relevant content identifiers to cause the new content to be provided to the device, and to cause the old content to be removed.

[0009] In accordance with the present invention, a database is provided that enables a number of elements

Nintendo Exhibit 1003
Part 1 of 2
Page 00591

to be stored as a hierarchical structure, with at least one of the elements representing a device to which content is to be distributed. Content identifiers identifying particular content may then be associated with elements in the hierarchical structure. Further, a server is provided which is able to reference the hierarchical structure in the database in order to generate a profile for a particular device, the profile containing a number of content identifiers, each content identifier identifying a content to be provided to that device. A device manager associated with the device is then able to act upon receipt of the profile to cause the content indicated by the profile to be provided to the device. with a record being kept identifying the content provided to the device in accordance with the profile. The record is preferably stored in a logically local storage area relative to the device, i.e. in a location that the device is always able to read irrespective of whether it is connected to a network.

[0010] The device manager may be stored on the device, or may be remote from the device. However, in the latter case, there will typically be something resident on the device itself to cause the device manager to execute, for example some configuration information.

[0011] In accordance with the present invention, when at some later point the device manager receives a subsequent profile from the server, it is arranged to compare the content identifiers in that subsequent profile with the record kept to identify the content provided to the device in accordance with a previous profile in order to determine new content not yet provided on the device and old content no longer to be provided on the device. The new content can then be retrieved to the device, whilst the old content is removed, for example by actually deleting that content, or by removing pointers to it in the local memory of the device.

[0012] By this approach, the system of the present invention is able to support a wide variety of different devices that may spend greater or lesser amounts of time connected to a network and which may need to store content locally in order to facilitate its use whilst not connected to the network. It should also be noted that the system also supports use with devices that may be permanently connected to the network. Through use of the present invention, the content provided to a device can be centrally managed such that once a content identifier has been associated with the appropriate element in the hierarchical structure, then that content identifier will be included in any profiles subsequently prepared for relevant devices, whereby the corresponding device manager for such a device will cause that content to be provided to the device the next time the profile is received. However, given that the content is not merely maintained centrally and accessed at that central point by the devices, but instead will typically be provided to the devices. the present invention further facilitates the removal of old content from a device through the comparison of a subsequent profile distributed by the server with a record kept to identify the content on that device that has been provided in accordance with a previous profile.

[0013] It should be noted that in preferred embodiments the present invention does not inhibit a user of a device from also installing their own content on the device since such content would not be included in the profiles, and so would not be provided to the device. or removed from the device, under the control of the device manager. However. the present invention does enable the distribution of certain core content to devices to be managed such that that content may be provided and subsequently removed in a structured manner without the need to involve the user of the device.

[0014] The content identifier may take a variety of forms. However, in preferred embodiments, each content identifier provides a name for the corresponding content, and a location indicator identifying a location from which that content can be obtained. Hence, when the device manager is seeking to obtain a content for the device, the location indicator in the corresponding content identifier can be used to determine the location from which the content can be obtained. In preferred embodiments. the name is not needed for the content retrieval process, but provides a descriptive reference for a network manager responsible for managing the hierarchical structure on the database, and indeed for the user of the device to which the content is retrieved.

[0015] The system in accordance with preferred embodiments of the present invention may be used to manage the distribution of a plurality of different types of content. Hence, preferably, the content identifier further identifies the type of the corresponding content. This information is then available for reference by a network manager responsible for managing the hierarchical structure on the database. This may. for example, provide a useful sanity check to enable the network manager to ensure that content is only allocated to devices able to receive that type of content.

[0016] It will be appreciated that the location identifier can take a variety of forms. provided that it serves to identify the location from which the content can be obtained. In preferred embodiments, the content is stored on servers contactable via the Internet. and the location indicator is a URL address.

[0017] It will be appreciated that when a content is provided to the device. some predetermined action will need to be taken by the device in order to correctly receive and store the content. The system of preferred embodiments of the present invention facilitates this by providing a number of packagers for associating with a content information required to handle the content when received by the device. Hence. when a content is retrieved to the device using a content identifier in the profile. the device not only receives the content but also any related information required to ensure correct handling of the content within the device. This content and related information provided to the device will be referred to hereafter as "a package".

[0018] As mentioned earlier, the distribution of a plu-

Nintendo Exhibit 1003
Part 1 of 2
Page 00592

rality of different types of content may be managed by the system. Accordingly, in preferred embodiments, a packager is provided for each type of content.

[0019] It will be appreciated that the information provided within the package to describe how the content should be handled can take a variety of different forms, depending on the content itself. For example, if the content is a data file for a particular application, for example a Microsoft Word file, then the package will identify the content as being of that type, and the type information can be used by the device manager to determine whether an installer exists for installing content of that type. If not, the content would typically just be stored in a default location, for example one specified by the device manager. However, if an installer is available, then that will be used to install the content on the device. Assuming an installer is to be used, the information in the package may also identify the required version number of Microsoft Word that is required to read the file. The installer would then try to locate that version of Word, and, for example, warn the user of the device if it is not found.

[0020] As another example, if the content is an application program. then it will generally need to be appropriately installed on the device by an installer. In such cases. in preferred embodiments, the information associated with such content may comprise an identification of which file is the main executable file, an identification of an icon to be used to represent the program on the desktop, etc. The relevant installer can then use that information to enable it to correctly install the application program.

[0021] It will be appreciated that since devices may be changed over time. and/or the use of any particular device may change over time, which may necessitate the association of different content with the device, it is necessary to be able to efficiently manage the hierarchical structure in the database in order to take account of such changes. Accordingly, the system of preferred embodiments has a management tool for providing an interface to enable a user to manage the hierarchical structure stored on the database. Hence, for example, if the hierarchical structure is used to represent a large number of devices within an organisation, a user in the form of a system administrator may use the management tool to manage the hierarchical structure to ensure that each device continues to be represented at an appropriate point in the hierarchical structure so that that device will receive the content that it is desired to provide to that device.

[0022] It will be appreciated that there are many different ways in which the hierarchical structure may be developed. However, in preferred embodiments, said elements within the hierarchical structure include one or more divisions, each division representing a logical grouping for devices, the management tool enabling divisions to be created and deleted, and enabling content identifiers to be associated with each division. Accordingly, at the top of the hierarchical structure, it is possible for a generic division to be provided within which all devices will fall, and then for particular divisions to be created depending from that generic division. For example, a technical support division may be provided to include all devices used by technical support staff, whilst a separate customer support division may be created to include all devices used by customer support staff. It should be noted that the user. e.g. the system administrator, is able to create and delete divisions as and when required in order to develop an appropriate hierarchical structure within which to categorise the devices to be represented within the hierarchical structure.

[0023] It should be noted that since content identifiers can be associated with each division, content that is to be common for all devices within a particular division need not be specified individually for each device, but rather can merely be specified once in connection with the corresponding division. In preferred embodiments, the profile generated by the server contains any content identifiers associated with the device and any content identifiers associated with a division from which the device depends in the hierarchical structure. It will be appreciated that this significantly improves the efficiency with which content can be associated with any particular device. Further, if a device is moved from one division to another. then the next time a profile is generated for that device, it will automatically receive an updated profile indicating the content that is relevant to that device in its new role. Any new content will then automatically be retrieved, whilst old content will be removed.

[0024] In preferred embodiments of the present invention. the management tool enables person identifiers identifying individuals to be provided as elements in the hierarchical structure, whereby the management tool can be used to associate, within the hierarchical structure, the device with the individual owning that device. The inclusion of this extra classification is useful, since often a particular individual in an organisation may have more than one device, and may submit requests for each of his/her devices to be provided with particular content. Since the individual devices can then depend from the relevant person identifier in the hierarchical structure, it is straightforward for the system administrator to then associate that new content with each device. Further, as individuals move around within the organisation, the system administrator is able to move the relevant person identifier between divisions. This will automatically cause all of that person's devices to also move, and for the relevant content for those devices to then be provided the next time that a profile is provided to those devices.

[0025] It will be appreciated that there are a number of mechanisms which could be used to provide the profile to the devices at predetermined intervals. For example. if a device is permanently connected to the network. then the server could be arranged to generate the profile at periodic intervals. However, in preferred embodiments, the system supports devices of many different

Nintendo Exhibit 1003
Part 1 of 2
Page 00593

types, at least some of which may not be permanently connected to the network. Given this situation, it is hence necessary for the profiles to be generated and distributed as and when the device is connected to the network. Accordingly, in preferred embodiments. the device manager is arranged to make a connection with the server at predetermined intervals in order to request the profile, the device manager identifying the device for which the profile is required.

[0026] Hence. for example, the device manager may request the profile immediately after the device has been powered, such an approach being suitable for bandwidth restricted devices that can only operate with the availability of a network. e.g. GSM receivers. Alternatively, the device manager may request a profile immediately after a network connection has been established, such an approach being suitable for those devices that are fully operational without network availability, but are assumed to make occasional connections, e.g. portable computers. Alternatively, as another example, the device manager may be arranged to request the profile on a periodic basic after discrete time intervals, such an approach being suitable for high bandwidth, permanently connected devices, for example cable television receivers and network computers.

[0027] As mentioned earlier, the distribution of a plurality of different types of content may be managed by the system. In preferred embodiments, at least one of the types is computer programs.

[0028] The database used to store the hierarchical structure may take a variety of forms. However, in preferred embodiments, the database is a relational database. It should be noted that in this preferred embodiment, this database is entirely separate to any directory services database that may also be provided as a "White Pages" database for resources within an organisation. It has been found to be beneficial to keep this database separate to the directory services database, since this frees the database from being bound by the structure already present in the directory services database. Instead, whilst certain details about resources in the organisation may be obtained from the directory services database for use in the database used to manage content distribution, the actual hierarchical structure within the database is then free to be determined having regard solely to the devices to be managed, and the content to be distributed. This enables a very efficient hierarchical structure to be generated.

[0029] Viewed from a second aspect, the present invention provides a computer program product providing a computer program operable to configure a server for use in a system according to the first aspect of the present invention, the computer program being arranged in operation to cause the server to perform the steps of: accessing a database providing a number of elements as a hierarchical structure of devices, content identifiers being able to be associated with elements in the hierarchical structure, and one of the elements representing a device to which content is to be distributed; and referencing the hierarchical structure in the database to generate a profile for the device, the profile containing a number of content identifiers indicating content to be provided to the device, the profile containing any content identifiers associated with the element representing the device, along with any content identifiers associated with elements in the hierarchical structure from which that element depends.

[0030] In one embodiment, the computer program product is further operable to configure a computer to provide an interface to enable a user to manage the hierarchical structure stored on the database.

[0031] In one embodiment, the computer program product is further operable to configure a computer to associate with a content information required to handle the content when received by the device.

[0032] Viewed from a third aspect, the present invention provides a computer program product providing a computer program operable to configure a device manager of a device for use in the system according to the first aspect of the present invention, the system having a database providing a number of elements as a hierarchical structure of devices, content identifiers being able to be associated with elements in the hierarchical structure, and one of the elements representing the device, the computer program being arranged in operation to cause the device manager to perform the steps of: receiving a profile from a server, the profile having been generated by referencing the hierarchical structure in the database to generate a profile for the device, the profile containing a number of content identifiers indicating content to be provided to the device, the profile containing any content identifiers associated with the element representing the device, along with any content identifiers associated with elements in the hierarchical structure from which that element depends; using the content identifiers in the profile to cause the content indicated by the profile to be provided to the device; upon receipt of a subsequent profile from the server, comparing the content identifiers in the subsequent profile with a record identifying the content provided to the device in accordance with a previous profile to determine new content not yet provided on the device and old content no longer to be provided on the device, and using the relevant content identifiers to cause the new content to be provided to the device, and to cause the old content to be removed.

[0033] Viewed from a fourth aspect, the present invention provides a method of managing distribution of content to a device, comprising the steps of: storing in a database a number of elements as a hierarchical structure of devices, content identifiers being able to be associated with elements in the hierarchical structure, and one of the elements representing the device; referencing the hierarchical structure in the database to generate a profile for the device, the profile containing a number of content identifiers indicating content to be

Nintendo Exhibit 1003
Part 1 of 2
Page 00594

provided to the device, the profile containing any content identifiers associated with the element representing the device, along with any content identifiers associated with elements in the hierarchical structure from which that element depends; with reference to the content identifiers in the profile, causing the content indicated by the profile to be provided to the device; maintaining a record identifying the content provided to the device in accordance with the profile; upon receipt of a subsequent profile, comparing the content identifiers in the subsequent profile with the record to determine new content not yet provided on the device and old content no longer to be provided on the device, and using the relevant content identifiers to cause the new content to be provided to the device, and to cause the old content to be removed.

Brief Description of the Drawings

[0034] The present invention will be described further, by way of example only, with reference to a preferred embodiment thereof as illustrated in the accompanying drawings, in which:

Figures 1A, 1B and 1C are block diagrams providing schematic illustrations of embodiments of the present invention;
Figure 2 is a further block diagram providing an architectural overview of a system in accordance with preferred embodiments of the present invention;
Figure 3 illustrates in more detail the connections to the server in accordance with preferred embodiments of the present invention;
Figures 4 to 8 illustrate a user interface used in preferred embodiments of the present invention to enable a system administrator to manage the hierarchical structure stored on the database;
Figures 9 and 10 provide an illustration of simplified examples of the hierarchical structure that may be stored within the database;
Figure 11 is a flow diagram illustrating the steps performed within a network device to request a profile, and act upon the profile when received;
Figure 12 is a flow diagram illustrating the steps performed within the server in order to provide a profile to the client;
Figures 13A to 13D are flow diagrams illustrating in more detail the procedure performed within a network device in order to act upon a received profile from the server;
Figure 14 is a flow diagram illustrating in more detail how the profite is prepared by the server in accordance with preferred embodiments of the present invention; and
Figure 15 provides a schematic illustration of how packagers are used in preferred embodiments to package content for distribution.

Description of a Preferred Embodiment

[0035] In the past, a relatively static number of fixed computer devices were managed by a localised support structure able to configure the complex desktop environments. The future, however, presents us with the prospect of having a profusion of devices, whether they be computer devices, or other electronic devices such as mobile phones, personal digital assistant devices (PDAs), electronic organisers, etc. which may or may not be geographically fixed. This will require an alternative management system which is more flexible.

[0036] The preferred embodiments of the present invention aim to provide such an alternative management system for distributed management of network devices within a network. The term "network device" as used herein is intended to refer to a device whose content is managed by the system of preferred embodiments of the present invention, but is not intended to imply that any such device is permanently connected to a network. For the purposes of preferred embodiments of the present invention, it is sufficient that any such "network device" is capable of making at least occasional connections to a network, either directly or via some other device. For example, certain devices may delegate their management to other devices which in turn must be able to make occasional network connections. For example, certain PDA-style devices are not inherently networkable, but rely on a PC to do certain things for them, such as install new programs. Since the PC can make occasional network connections, such PDAs will also be "network devices" which can be managed by the system in accordance with preferred embodiments of the present invention.

[0037] Each network device is in preferred embodiments provided with a client program (which may alternatively be referred to herein as a device manager) which is arranged to communicate with a server, the server maintaining details of content (for example, programs or data) desired to be present on each device. In preferred embodiments. the client program identifies to the server the network device. and the server sends a profile of the content desired to be present on that device. The client program then preferably configures the network device so that it contains the content identified in the profile, any content not currently present on the device, but identified in the profile. being retrieved in a predetermined manner.

[0038] In preferred embodiments of the present invention. the client program and server operate on the Java™ platform. The ubiquity of Java™ across platforms as various as cable television receivers and mobile telephones, allows the possibility to centrally control almost any kind of device entirely remotely, provided that at least occasional successful network connections are established to enable that control to take place.

[0039] In preferred embodiments of the invention, the client program on each network device is responsible

Nintendo Exhibit 1003
Part 1 of 2
Page 00595

for autonomously updating the device's configuration. Dependent on the kind of device, the client program executes at defined intervals. namely either:

1. immediately after the device has been powered;
2. immediately after a network connection has been established; or
3. after discrete time intervals.

[0040] The first scenario is designed for bandwidth restricted devices that can only operate with the availability of a network, e.g. GSM receivers. The second will be used for those devices that are fully operational without network availability, but are assumed to make occasional connections e.g. portable computers. The third scenario is designed for high bandwidth, permanently connected devices like cable television receivers and network computers.

[0041] The client program communicates the identity of the device to a server, which replies with a profile of content (for example programs or data) that are desired by the network authority to be present on this device. The server does not transmit the content, rather the location from which each one can be retrieved. The client records each content it fetches, so is able to selectively fetch new or updated content, and delete content nolonger required, thus abrogating all responsibility of the device user to manage the device.

[0042] The network authority is the entity with responsibility for defining the profile of the devices. This task is made simpler through the use of a hierarchical definition/structure, i.e. each device is represented as a member of a logical grouping called a division. Each division may in turn be a member of another division. in the manner of a linear tree, until the common ancestor is reached. A profile may be defined for each division. Thus a profile for a device consists of any content explicitly designated to it within the hierarchical definition, plus that of its division. plus the parent division and so on until the root division. For example, with reference to Figure 10, where device names are enclosed with brackets. the profile of Adelie is defined not only by its own configuration, but also that of Penguin. Bird and All. Therefore. if Adelie became part of the Gull division, it would still inherit the configuration of Bird and All but would now include that of Gull rather that Penguin.

[0043] Schematic overviews of example embodiments of the system of the present invention are illustrated in Figures 1A to 1C.

[0044] Figure 1A illustrates one possible embodiment of the present invention, in which a number of network devices 10 are linked via a LAN 50 with a server 30. In this embodiment, the network devices are likely to be PCs, but need not be, and indeed could be any other suitable electronic device, for example a router, an intelligent hub, etc. Further, the network devices could be personal organisers, PDAs, etc., which may connect to the network via a PC.

[0045] The server 30 is connectable to a database 40 containing a hierarchical definition identifying the devices and the content to be associated with those devices. A system administrator can manage the hierarchical definition by connecting to the server 30 via a system administration device 20. The location of the system administration device can be varied, but in the Figure 1A example, the system administration device is connected to the server via the LAN 50.

[0046] Each network device 10 will in preferred embodiments have a client program installed thereon and arranged to communicate with the server 30 in order to obtain a profile for the respective network device, the profile being derived by the server having regard to the hierarchical definition. Hence. the system in accordance with figure 1A provides for the distributed management of those network devices, since the hierarchical definition is maintained centrally, and then client programs are distributed amongst the relevant network devices. Further, the hierarchical definition can be directly managed from the server, or alternatively can be managed from some distributed point, such as the system administration device 20.

[0047] Figure 1B provides an illustration of an alternative embodiment in which the present invention may be used. In this embodiment, the network devices are connected via a mobile telecommunications network, and the network devices 10 will be electronic devices arranged to communicate over the mobile network, for example mobile phones, or laptop computers with mobile telecommunication capability. In this embodiment, the server 30 is connected via a telecommunications infrastructure 60 to a number of transmitters/receivers 70 used to communicate with the network devices 10. The system operates in basically the same way as that described with reference to figure 1A, with each network device 10 being provided with a client program to enable it to communicate with the server 30. It should be noted that the system administration device used by the system administrator to manage the hierarchical definition within the database 40 may be anywhere within the network, and hence may be on the server 30, or may indeed be provided by a network device anywhere within the telecommunications network.

[0048] In preferred embodiments of the present invention, many different types of devices may be managed, which may connect to the server 30 via different mechanisms. This is schematically illustrated by the embodiment shown in Figure 1C. Here, certain network devices 100, for example desktop systems, may connect to the server directly via an Ethernet connection 130. Further, other network devices 110, for example pocket organisers, mobile telephones, etc. may connect to the server via wireless communications with a transmitter/receiver 70. In addition, other network devices 120, for example a laptop computer or a multimedia PC, may connect to the server via the Internet 140.

[0049] As mentioned earlier, the system of preferred

Nintendo Exhibit 1003
Part 1 of 2
Page 00596

embodiments is available for devices that support at least occasional network connections. In preferred embodiments, the system uses Java and Internet technologies to enable the remote management of a diverse range of devices. Figure 2 provides an illustration of the architectural overview of the system of preferred embodiments. The server 30 uses Java's Remote Method Invocation (RMI) and Jini connectivity to make itself available to client programs 200 as a configuration service. RMI is a Java mechanism that allows two programs to communicate transparently over a network. Jini is a software infrastructure that allows services to be made available across the network. the reader being referred to the website http://www.sun.com/jini/ for more details.

[0050] Further, the server uses standard Internet protocols such as HTTP or FTP to distribute content. Hence, as illustrated in Figure 2, a client program 200 resident on a network device may connect to the server 30 via either RMI 220 or Jini 230 mechanisms in order to request and receive a profile from the server. Further, a management tool 210 (preferably a computer program) on a system administrator's device may, for example, use an RMI mechanism 220 to assign new content to elements (e.g. divisions, devices) within the hierarchical structure maintained on the database 40. Additionally, when the profile has been received, the client program 200 may collect content from servers 250, 260 via the Internet 240 using the standard Internet protocols such as HTTP or FTP as appropriate.

[0051] It should be noted that the system of the preferred embodiment is a highly distributed application. The database 40, the server 30, the management tool 210, and indeed any directory server that may be used to obtain information to use within the database 40, can all be located on separate machines.

[0052] Figure 3 provides more details of the way in which the server is connected in accordance with preferred embodiments of the present invention. The server 30 is designed to integrate with existing servers. Hence, a database back-end 40 can be used to store the hierarchical structure used by the server to generate profiles for network devices. Java Database Connectivity (JDBC) facilitates the connection of third-party databases to the server 30. More information concerning JDBC can be found at the web address http://java.sun.com/products/jdbc/.

[0053] Further, a standard directory server, such as LDAP (an Internet standard directory server), NDS, etc., can be connected to the server 30 to allow information about particular users within the organisation to be obtained by the server 30. As illustrated in Figure 3, Java Naming and Directory Interface (JNDI) allows different types of directory servers to be connected to the server 30. For more information about JNDI, the reader is referred to the web address http://java.sun.com/products/jndi/. Whilst it is clear that the hierarchical structure in the database 40 could be created from scratch by the server 30. it is quite likely that an organisation wishing to have their devices managed in accordance with the system of preferred embodiments of the present invention will already have a directory server giving relevant details about the users, etc. Hence, the task of creating the hierarchical structure in the database 40 can be significantly simplified by allowing the server 30 to obtain relevant details about users, etc. from any standard directory server already provided within the organisation.

[0054] Further, it has been found to be highly desirable to store the hierarchical structure used to manage the distribution of content to devices in an entirely separate database 40, rather than by seeking to incorporate the additional information within the rather fixed structure of an existing directory server database, since this facilitates far more flexibility in the creation of appropriate divisions. and locations of devices within divisions, having regard to the devices to be managed, and the content to be distributed to those devices.

[0055] In preferred embodiments, standard Internet servers 250 and 260 are then used to store the actual content to be distributed to the devices. The server 30 is then able to communicate with the servers 250, 260, for example via standard Internet connections, to check where content is stored, and to check the format in which that content is stored, etc.

[0056] As illustrated in Figure 3, a standard RMI registry and an optional Jini djinn are used to make the service available to network devices. An RMI registry is a remote program that provides mechanisms for locating other remote programs, and hence facilitates the use of the RMI mechanism to enable client programs to communicate with the server 30. Djinn is the name given to the group of devices, resources and users joined by the Jini software infrastructure.

[0057] Considering now the client programs 200 associated with particular network devices. these client programs can connect to the server using one of two methods depending on their configuration. For network devices with built-in client code. Java's RMI mechanism can be used, whilst dynamic, downloadable client software is provided as an alternative through the optional Jini service. Using the Jini approach. a device will already have what is known as a service browser which searches for services that are available. In this case, the client program is not installed locally on the device. but the process may be automated through use of an appropriate configuration present on the device.

[0058] On each network device, a small client registry is maintained keeping a record of all content present on the device that has been obtained in accordance with a profile received from the server 30. When the server is contacted, a profile describing what should be present on the device is retrieved. As will be described in more detail later, the new and updated content indicated by the profile is retrieved and defunct content is removed. During this process, any installers and de-installers are preferably automatically downloaded from the server 30 and invoked. It should be noted that all of this happens

without any involvement from the user of the network device.

[0059] In preferred embodiments, a management tool application is provided to present a simple graphical interface to assist an administrator or the like, to enable the system administrator to build and maintain a hierarchical structure of divisions and devices within the database 40. Content identifiers can then be dragged and dropped on to particular elements representing divisions and/or devices in order to associate content with the elements of the hierarchical structure. Via integration with a standard directory server as illustrated earlier with reference to Figure 3, the system administrator is able to determine who owns a particular device on the network. Hence, equipping a person's device for a new role simply involves dragging an icon representing that person to a new division. These concepts will be illustrated further with reference to Figures 4 to 8, which provide example illustrations of the graphical interface provided by the management tool to enable a system administrator to manage the hierarchical structure maintained by the server 30 on the database 40.

[0060] With reference to figure 4, the left hand window provides a schematic illustration of the hierarchical definition, whilst the right hand window serves as an information display area. The window at the bottom of the screen contains a list of content identifiers that are available for allocation to elements of the hierarchical structure representing particular devices or divisions (in this example the content being computer programs). As can be seen from Figure 4, each content identifier includes a name for the content, and a location indicator, in this case a URL address. identifying the location from which the corresponding content can be retrieved. Optionally, the content identifier may include information such as version numbers. type of content, and the date last modified.

[0061] Figure 5 shows the information that will be displayed when the system administrator selects the "Engineer" division. As can be seen from the information display area. this indicates that the programs "yellow", "indigo" and "orange" are associated with the division "Engineer", and that also the operating system "green" and the application "red" are inherited from the division "All".

[0062] Figure 6 illustrates the information provided if the system administrator were to select an individual, in this case the individual Nigel Brookes, who has two devices associated with him, namely "Hugh" and "Cuthbert". Finally, Figure 7 illustrates the programs associated with the device "Hugh". It can be seen that the device "Hugh" has the application "violet" associated directly with it, but also inherits the programs associated with the divisions "Engineer" and "All".

[0063] Figure 8 illustrates the graphical interface that may be provided for an alternative example database structure. Here, a device called Future Phone is indicated as belonging to an individual, Nigel Brookes, who is allocated within the Engineers division, which itself is a division of the Concept Technologies Division. Further, the Concept Technologies Division is contained within the Hugh Symons Division. which is contained within the All Division. As can be seen from Figure 8, the device Future Phone has two applications associated therewith, and also inherits an application from the division All. In this instance, it is clear that the divisions Hugh Symons, Concept Technologies and Engineers do not have any content associated directly with them, since otherwise the device Future Phone would also have inherited the content from those divisions.

[0064] With reference to Figure 8, it will also be seen that the content identifiers in this case also include optional information identifying a default lease period. This information enables the client program on a network device to automatically remove the content after the lease period expires. Hence, with reference to Figure 8. it can be seen that two of the applications allocated to the device Future Phone are on a perpetual lease, but that the application JarBall Madness is on a thirty day lease expiring on 26 August 1999. The client program can use this information to automatically remove JarBall Madness from the Future Phone device on that date.

[0065] For completeness, Figure 9 is also provided to give a simple illustration of a portion of a hierarchical structure that may be maintained within the database 40. As mentioned earlier, devices are organised into logical, hierarchical groupings called divisions. Each division inherits the contents of its parent division. Content can be assigned to these divisions, and to individual devices, which then facilitates the generation of a profile for particular devices.

[0066] In Figure 9, we can see that Sue Bar owns the device "My Cell Phone". She is part of the Customer division and also the Support and All divisions. Her device will therefore have the content assigned to All, Support, Customer and to that specific device. If Sue decided that she would like to make use of a service that will send all SMS (Short Message Service) messages to her e-mail account, she can request that service from the relevant system administrator. The system administrator may decide not to make this service generally available, and so instead will assign it to her cell phone only. When that device next retrieves a profile from the server, it will automatically receive the relevant application.

[0067] The system administrator retains responsibility for the entire hierarchy, but is able to delegate the control of sub-divisions to other managers. Hence, referring to Figure 9, the network administrator could retain responsibility for the All division, but may choose to delegate the management of the Customer Support division and the Technical Support division to one or more different managers.

[0068] The flow diagrams of figures I 1 and 12 provide a brief illustration of the process performed when a client program on a device is executed in accordance with one embodiment of the present invention, figure 11 illustrat-

Nintendo Exhibit 1003
Part 1 of 2
Page 00598

ing the processing steps executed by the client program, and figure 12 illustrating the processing steps executed by the server. It is clear that not all embodiments need to execute the exact sequence of steps illustrated in figures 11 and 12, but rather figures 11 and 12 are intended to illustrate a particular embodiment. For example, if the server determines that the device is not currently in the database, then it may be arranged to refuse that device access to the network, rather than creating a new entry for that device in the "new devices" division.

[0069] With reference to the embodiment of figure 12, it will be appreciated that if a "new devices" division were provided, it would generally be provided as a child of the division "All". If any content is associated with the division "All" then this new device will inherit that content. However, alternatively, both the divisions "All" and "new devices" may be arranged to have no content associated with them, such that the new device is not provided with any content at the time that it first contacts the server.

[0070] Irrespective of which approach is taken, in preferred embodiments the network administrator would seek to reallocate any devices placed within the "new devices" division to the appropriate division within the hierarchy. For example, having reference to figures 4 to 7, if the new device was actually within the "Support" division, then the support administrator would move that device from the "new devices" division to the "Support" division, so that in subsequent accesses, that new device will be arranged to receive the content appropriate to the "Support" division.

[0071] Figures 13 and 14 are flow diagrams providing a more detailed illustration of the process that may be performed when a client program on a device is executed. Figures 13A to 13D can be considered as a more detailed illustration of the embodiment illustrated in Figure 11, whilst Figure 14 illustrates a different embodiment to that illustrated in Figure 12, in that rather than allocating unknown devices to a new devices division, the process illustrated in Figure 14 merely terminates the process, and hence the process can only be used once devices have been allocated by the system administrator to an appropriate location in the hierarchical structure.

[0072] With reference to Figure 13A, when the client program executes, it starts at step 500, and proceeds to step 510, where it is determined whether there is any available network. If not, the process terminates at step 520, and the process will begin again next time that the client program executes. As mentioned earlier, the client program is preferably arranged to execute at predetermined intervals, these intervals being determined dependent on the type of device.

[0073] If the network is available, then the process proceeds to step 530 where the device seeks to download the profile from the server 30. At step 540, it is determined whether the download process has been successful, i.e. whether a profile has been received from the server, and if not, the process loops back to step 530. It will be appreciated that if there is some temporary problem with either the server or the network which inhibits the profile from being delivered to the client program, then the client program could stall at this point. Accordingly, it may be appropriate in some embodiments to provide a time-out mechanism here, whereby the process branches to step 520 if no successful downloading of the profile has been achieved within a predetermined time. However, for simplicity, this process has not been illustrated in Figure 13A.

[0074] Assuming the profile downloading is successful, then the process proceeds to step 550, where the new profile is compared with a content record 560 maintained on the network device to identify the content retrieved to the device in accordance with a previous profile. However, prior to discussing the rest of Figure 13A to Figure 13D, the manner in which the profile is generated by the server 30 will now be described with reference to Figure 14. The profile generation is preferably performed by software installed on the server 30. The process begins at step 700, and at step 705 the server waits for a device connection. Once the device has connected, it is determined at step 710 whether the device is known, i.e. whether it is represented in the hierarchical structure, and if not, the connection is closed at step 720. The process then returns to step 705 to await a further device connection.

[0075] However, assuming that the device is known, then the process proceeds to step 715 where the content identifiers for that device are retrieved from the corresponding element in the hierarchical structure maintained on the database 40. Then, at step 725, it is determined which division the device is contained within in the hierarchical structure, and then the content identifiers associated with that division are also added to the content identifiers retrieved at step 715.

[0076] Next, at step 735, it is determined whether the division has a parent within the hierarchical structure, and if so, that parent division is retrieved at step 730, and the content identifiers within that division are then added at step 725 to those content identifiers already retrieved from the database. This process continues until it is determined at step 735 that the current division has no parent (i.e. with reference to the earlier examples, this will mean that the current division is the All division), at which point it is determined that all appropriate content identifiers have been located. Accordingly, these content identifiers are sent to the device at step 740 as the requested profile. The process then returns to step 705 to await a further device connection.

[0077] Returning to Figure 13A, as a result of step 550, any new content to be retrieved, old content to be deleted, or content to be updated, will have been determined through the comparison of the new profile with the previously stored content record 560. Accordingly, the process proceeds to step 570 in Figure 13B, where it is determined whether there is any content to remove.

Nintendo Exhibit 1003
Part 1 of 2
Page 00599

If so, it is determined at step 575 whether it is appropriate to execute an uninstaller in order to remove the content.

[0078] Before continuing with the description of Figure 13B, the mechanism for determining whether an installer/uninstaller is required will be discussed in more detail. As mentioned earlier, when the content is retrieved to the network device, it preferably also includes related information identifying how that content should be handled upon receipt. In accordance with preferred embodiments of the present invention, the association of this further information with the content is achieved via one or more packagers provided by the system of preferred embodiments, these packagers preferably being embodied as computer programs. This process is illustrated schematically in Figure 15.

[0079] The content delivery mechanism is very flexible, allowing developers to introduce new types of content along with any necessary installers and uninstallers without having to change any client-side software. For example, all of the sales force in a particular organisation could have the latest performance results provided to their devices and automatically installed into a database application on those devices.

[0080] This flexibility is achieved by bundling content up in standard Java archives (JAR files) which in preferred embodiments have associated therewith a well-known file "META-INF/manifest.mf". and passing those Java archives through a packager as illustrated in Figure 15. A JAR file is a file or files that have been compressed into a single file using a jar tool supplied with the Java Development Kit.

[0081] As illustrated in Figure 15, the content 800 is passed to an appropriate packager within a group of packagers 810. For example, a particular packager 830 may be provided for packaging applications, a different packager 840 may be provided for packaging documents, and a further packager 850 may be provided for packaging other type of content. The relevant packager alters the content of the manifest file to include at least the name, type and version of the content. The packager is also at liberty to include in this file any other variable which may be required. This results in a package 820 which can be distributed to network devices in accordance with preferred embodiments of the present invention. It should be noted that the resulting package is still completely compatible with Java.

[0082] A packager is in preferred embodiments provided for each type of content. In addition, each type of content may optionally have an installer/uninstaller provided to install/uninstall such content on a network device. Since the packagers are type specific, and since any installers/uninstallers are also type specific, it will be apparent that the packager can be arranged to include any variables specifically required by the corresponding installer/uninstaller. For example, if the content type is Microsoft Word documents for PCs, the packager might include within the package the required version number of Microsoft Word that is required to read the file. The installer would then try to locate that version of Word, and, for example, warn the user of the device if it is not found.

[0083] As another example, if the content type is an application program, the packager might include within the package an identification of which file is the main executable file, an identification of an icon to be used to represent the program on the desktop, etc. The relevant installer can then use that information to enable it to correctly install the application program.

[0084] Hence, it can be seen that depending on the content type, an installer/uninstaller may or may not be needed. The package as retrieved specifies, amongst other things, the content type, as indeed does the content identifier in the profile, and hence the device manager can check to see if an installer/uninstaller is associated with that content type. This may, for example, be appropriate if the content is an application program.

[0085] Returning to Figure 13B, if it is determined at step 575 that an uninstaller should be executed, then the process proceeds to step 585, where the appropriate uninstaller is downloaded and executed in order to remove the relevant content. In preferred embodiments, to download the appropriate uninstaller, the client program asks the RMI registry 310 illustrated in Figure 3 whether an installer/uninstaller exists for the type of content received. If such an installer/uninstaller exists, it will be downloaded by the RMI registry to the client program, whereafter it can be executed to uninstall the particular content in question.

[0086] However, not all content types will require an uninstaller. For example, the content may be a data file which merely needs deleting. In this event, it will determined at step 575 that it is not necessary to execute an uninstaller, in which case the process will proceed to step 580 where the content will be deleted. The process then returns to step 570, to determine whether any further content needs removing. If so, the above described process is repeated.

[0087] If not, the process proceeds to step 590, where it is determined whether there is any content to be updated. If so, the process proceeds to step 595, where the updated content is downloaded from the location indicated within the corresponding content identifier provided within the profile. As mentioned earlier, the content is preferably stored on Internet servers, and in this case, the content identifier will identify an appropriate Internet address from which to download the content. Once the content has been downloaded, it will be determined at step 600 in Figure 13C whether it is necessary to execute an installer and/or uninstaller, as mentioned above this decision being taken based on the type of content to be updated.

[0088] If, for example, the content is a data file, then it may not be appropriate to execute an installer and/or uninstaller, and accordingly the process will proceed to step 615, where the outdated content is deleted, and the

Nintendo Exhibit 1003
Part 1 of 2
Page 00600

updated content is saved. However, assuming it is determined that an installer and/or uninstaller are required, then the process proceeds to step 605 where any necessary installer and/or uninstaller is downloaded using the process described earlier with reference to step 585. The uninstaller can then be executed to remove the outdated content, whereafter the process proceeds to step 610, where the necessary installer is executed to install the updated content. The process then returns to step 590 to determine whether any further content needs to be updated. If so, the above described process is repeated, but if not, the process proceeds to step 620 shown in Figure 13D.

[0089] At step 620, it is determined whether there is any new content to be added. If so, then the process proceeds to step 625, where the new content is downloaded using the information provided in the relevant content identifier included within the profile. Then, at step 630 it is decided whether an installer needs to be executed and if so, the process proceeds to step 635, where the appropriate installer is downloaded and executed in order to install the content. If at step 630 it is decided that an installer is not required, then the process can proceed directly to step 640, where the new content is saved. With regard to the issue of where new content should be saved, if an installer is used, it may be arranged to determine if there is a default location for the storage of that type of content. For example, if the content is a Microsoft Word file, then the installer may review the configuration settings of the device to see if a default location for Microsoft Word files is specified, and if so that location will be used for the storage of the content. If no such default location exists, or if an installer is not used, the device manager may be arranged to specify a default location to which to store content.

[0090] Once the new content has been stored on the device, the process proceeds back to step 620, where it is determined whether there is any further content to be added. If so, the above described process is repeated, but if no further content is to be added, the process then proceeds to step 645, where the current profile is stored as the content record 560. In preferred embodiments, it is assumed that at this stage the device will contain all content as indicated in the current profile. However, in the event that for some reason the device was unable to retrieve any particular item of content in the profile, for example because the corresponding server was at that time out of action, then it is preferred that the content record 560 be updated to reflect the actual content retrieved to the device in accordance with the profile, rather than merely storing the current profile itself. Once the content record has been updated, then the process proceeds to step 655, where the process terminates.

[0091] From the above description, it will be appreciated that the system of preferred embodiments of the present invention provides a platform for managing disparate. heterogeneous. distributed devices. These devices include, but are not limited to computers, digital mobile telephones and set-top boxes. The system of preferred embodiments provides a unique mechanism for the automatic distribution. installation and removal of almost any kind of content, including applications, without any user intervention. A system administrator uses a management tool to build a program of content for each device or group of devices. At predetermined intervals, a small piece of client-side code compares a profile generated by the server with a record of the content stored on the device in accordance with the previous profile. Any new or updated content is automatically retrieved and installed and any defunct content is removed. In preferred embodiments, the server, management tool, and client program are all Java-based.

[0092] To illustrate the versatility of the above system, the following example scenarios can be considered.

[0093] Firstly, consider the situation where a member of a corporate network introduces a new device. In accordance with preferred embodiments of the present invention, during synchronisation, the device asks for the identity of the owner. The server establishes the presence of the user in the directory server and automatically installs the device as being owned by that user. The device will be assigned a profile based on its location in the hierarchical structure, and will automatically receive its appropriate content.

[0094] As a second example, consider the situation where a member of an organisational unit changes function. In preferred embodiments of the present invention, their user icon within the hierarchical structure is dragged and dropped on to the division representing their new function. The suite of content is then automatically updated to reflect the change the next time the profile is received by the user's device.

[0095] As a further example, consider the situation where a team operates a pool of mobile telephones. Normally, an organisational unit in the directory server owns these. When a user requests a device, it is dragged from the organisational unit on to the user's icon. The device will then automatically be provisioned with the content appropriate for that user.

[0096] As another example, consider the situation where a new program is to be introduced. A manager packages the new program using one of the packagers described earlier, moves the packaged content to a web server, and tells server 30 the network location of that content. A corresponding content identifier is then generated and associated with the appropriate divisions/devices within the hierarchical structure.

[0097] Finally, consider the scenario where a program is updated. Provided it is packaged in the appropriate manner using one of the earlier described packagers, it will be automatically distributed as an upgrade, and the upgrade will be installed in accordance with the process described earlier with reference to Figures 13A to 13D.

[0098] Although a particular embodiment of the invention has been described herewith, it will be apparent that

Nintendo Exhibit 1003
Part 1 of 2
Page 00601

the invention is not limited thereto, and that many modifications and additions may be made within the scope of the invention. For example, various combinations of the features of the following dependent claims could be made with the features of the independent claims without departing from the scope of the present invention.

Claims

1. A system for managing distribution of content to a device (10; 100, 110, 120), comprising:

   a database (40) for storing a number of elements as a hierarchical structure of devices, content identifiers being able to be associated with elements in the hierarchical structure, and one of the elements representing the device;
   a server (30) for referencing the hierarchical structure in the database to generate a profile for the device, the profile containing a number of content identifiers indicating content to be provided to the device, the profile containing any content identifiers associated with the element representing the device, along with any content identifiers associated with elements in the hierarchical structure from which that element depends;
   a device manager (200) associated with the device and arranged to receive the profile from the server and to use the content identifiers in the profile to cause the content indicated by the profile to be provided to the device, a record being kept identifying the content provided to the device in accordance with the profile;
   the device manager further being arranged upon receipt of a subsequent profile from the server to compare the content identifiers in the subsequent profile with the record to determine new content not yet provided on the device and old content no longer to be provided on the device, the device manager being arranged to use the relevant content identifiers to cause the new content to be provided to the device, and to cause the old content to be removed.

2. A system as claimed in Claim 1, wherein each content identifier provides a name for the corresponding content, and a location indicator identifying a location from which that content can be obtained.

3. A system as claimed in Claim 2, wherein the distribution of a plurality of different types of content are managed by the system, and the content identifier further identifies the type of the corresponding content.

4. A system as claimed in Claim 2 or Claim 3, wherein the content is stored on servers (250, 260) contactable via the Internet, and the location indicator is a URL address.

5. A system as claimed in any preceding claim, further comprising a number of packagers (810) for associating with a content information required to handle the content when received by the device.

6. A system as claimed in Claim 5, wherein the distribution of a plurality of different types of content are managed by the system, and a packager is provided for each type of content.

7. A system as claimed in Claim 5 or Claim 6, wherein the information associated with a content comprises an identification of an installer to be used to install the content on the device.

8. A system as claimed in any preceding claim, further comprising a management tool (210) for providing an interface to enable a user to manage the hierarchical structure stored on the database.

9. A system as claimed in Claim 8, wherein said elements include one or more divisions, each division representing a logical grouping for devices, the management tool enabling divisions to be created and deleted, and enabling content identifiers to be associated with each division.

10. A system as claimed in Claim 9, wherein the profile generated by the server contains any content identifiers associated with the device and any content identifiers associated with a division from which the device depends in the hierarchical structure.

11. A system as claimed in any of claims 8 to 10, wherein the management tool enables person identifiers identifying individuals to be provided as elements in the hierarchical structure, whereby the management tool can be used to associate, within the hierarchical structure, the device with the individual owning that device.

12. A system as claimed in any preceding claim, wherein the device manager is arranged to make a connection with the server at predetermined intervals in order to request the profile, the device manager identifying the device for which the profile is required.

13. A system as claimed in any preceding claim, wherein the distribution of a plurality of different types of content are managed by the system, and at least one of said types is computer programs.

14. A system as claimed in any preceding claim, where-

Nintendo Exhibit 1003
Part 1 of 2
Page 00602

in the database is a relational database.

15. A computer program product providing a computer program operable to configure a server (30) for use in a system as claimed in any preceding claim, the computer program being arranged in operation to cause the server to perform the steps of:

accessing a database providing a number of elements as a hierarchical structure of devices, content identifiers being able to be associated with elements in the hierarchical structure, and one of the elements representing a device to which content is to be distributed; and
referencing (470) the hierarchical structure in the database to generate a profile for the device, the profile containing a number of content identifiers indicating content to be provided to the device, the profile containing any content identifiers associated with the element representing the device, along with any content identifiers associated with elements in the hierarchical structure from which that element depends.

16. A computer program product as claimed in Claim 15, further operable to configure the server to transmit (480) the profile to a device manager of the device.

17. A computer program product as claimed in Claim 16, wherein the profile is generated in response to a request for the profile from the device manager.

18. A computer program product as claimed in any of claims 15 to 17, further operable to configure a computer to provide an interface to enable a user to manage the hierarchical structure stored on the database.

19. A computer program product as claimed in Claim 18, wherein the elements in the hierarchical structure include one or more divisions, each division representing a logical grouping for devices, the computer program enabling divisions to be created and deleted, and enabling content identifiers to be associated with each division.

20. A computer program product as claimed in Claim 18 or Claim 19, wherein the computer program enables person identifiers identifying individuals to be provided as elements in the hierarchical structure, whereby the computer program can be used to associate, within the hierarchical structure, the device with the individual owning that device.

21. A computer program product as claimed in any of claims 15 to 20, further operable to configure a computer to associate with a content information required to handle the content when received by the device.

22. A computer program product providing a computer program operable to configure a device manager (200) of a device (10; 100, 110, 120) for use in a system as claimed in any of claims 1 to 14, the system having a database (40) providing a number of elements as a hierarchical structure of devices, content identifiers being able to be associated with elements in the hierarchical structure, and one of the elements representing the device, the computer program being arranged in operation to cause the device manager to perform the steps of:

receiving (410) a profile from a server (30), the profile having been generated by referencing the hierarchical structure in the database to generate a profile for the device, the profile containing a number of content identifiers indicating content to be provided to the device, the profile containing any content identifiers associated with the element representing the device, along with any content identifiers associated with elements in the hierarchical structure from which that element depends;
using the content identifiers in the profile to cause the content indicated by the profile to be provided (430) to the device;
upon receipt of a subsequent profile from the server, comparing (550) the content identifiers in the subsequent profile with a record (560) identifying the content provided to the device in accordance with a previous profile to determine new content not yet provided on the device and old content no longer to be provided on the device, and using the relevant content identifiers to cause the new content to be provided (625) to the device, and to cause the old content to be removed (580, 585).

23. A method of managing distribution of content to a device, comprising the steps of:

storing in a database (40) a number of elements as a hierarchical structure of devices, content identifiers being able to be associated with elements in the hierarchical structure, and one of the elements representing the device;
referencing (470) the hierarchical structure in the database to generate a profile for the device, the profile containing a number of content identifiers indicating content to be provided to the device, the profile containing any content identifiers associated with the element representing the device, along with any content identifiers associated with elements in the hierarchical structure from which that element depends;

Nintendo Exhibit 1003
Part 1 of 2
Page 00603

with reference to the content identifiers in the profile, causing the content indicated by the profile to be provided (430) to the device;
maintaining a record (560) identifying the content provided to the device in accordance with the profile;
upon receipt of a subsequent profile, comparing (550) the content identifiers in the subsequent profile with the record to determine new content not yet provided on the device and old content no longer to be provided on the device, and using the relevant content identifiers to cause the new content to be provided (625) to the device, and to cause the old content to be removed (580, 585).

Patentansprüche

1. System für die Verwaltung der Verteilung von Inhalt zu einer Einrichtung bzw. einem Gerät(10, 100, 110, 120), das aufweist:

eine Datenbank (40) für das Speichern einer Anzahl von Elementen als eine hierarchische Struktur von Einrichtungen, von Inhaltsidentifizierern, die mit Elementen in der hierarchischen Struktur verknüpft werden können, und von einem der Elemente, das die Einrichtung repräsentiert,
einem Server (30) für das Herstellen von Bezügen auf die hierarchische Struktur in der Datenbank, um ein Profil für die Einrichtung zu erzeugen, wobei das Profil eine Anzahl von Inhaltsidentifizierern enthält, die den der Einrichtung zur Verfügung zu stellenden Inhalt anzeigen, wobei das Profil alle Inhaltsidentifizierer, die mit dem Element verknüpft sind, das die Einrichtung darstellt, zusammen mit allen Inhaltsidentifizierern, die mit Elementen in der hierarchischen Struktur verknüpft sind, von denen dieses Element abhängt, enthält,
einen Einrichtungsmanager (200), der mit der Einrichtung verknüpft ist und derart angeordnet ist, daß er das Profil von dem Server empfängt und die Inhaltsidentifizierer in dem Profil verwendet, um zu veranlassen, daß der Inhalt, der von dem Profil angezeigt wird, der Einrichtung zur Verfügung gestellt wird, wobei ein Eintrag beibehalten wird, der den Inhalt identifiziert, der in Übereinstimmung mit dem Profil zu der Vorrichtung geliefert wurde,

wobei der Einrichtungsmanager weiterhin derart angeordnet ist, daß er mit Empfang eines nachfolgenden Profils von dem Server die Inhaltsidentifizierer in dem nachfolgenden Profil mit dem Eintrag vergleicht, um den noch nicht der Einrichtung bereitgestellten neuen Inhalt und den nicht länger der Einrichtung zur Verfügung zustellenden alten Inhalt bestimmt, wobei der Einrichtungsmanager derart angeordnet ist, daß er die relevanten Inhaltsidentifizierer verwendet, um zu veranlassen, daß der neue Inhalt der Einrichtung zur Verfügung gestellt wird und um zu veranlassen, daß der alte Inhalt entfernt wird.

2. System nach Anspruch 1, wobei jeder Inhaltsidentifizierer einen Namen für den entsprechenden Inhalt bereitstellt, und ein Ortsindikator einen Ort identifiziert, von dem dieser Inhalt erhalten werden kann.

3. System nach Anspruch 2, in dem die Verteilung einer Mehrzahl von unterschiedlichen Inhaltstypen von dem System verwaltet werden und der Inhaltsidentifizierer weiterhin den Typ des entsprechenden Inhaltes identifiziert.

4. System nach Anspruch 2 oder Anspruch 3, wobei Inhalt auf Servem (250, 260) gespeichert wird, die über das Internet kontaktierbar sind, und wobei der Ortsanzeiger eine URL-Adresse ist.

5. System nach einem der vorherigen Ansprüche, das weiterhin eine Anzahl von Packern (810) aufweist für die Verknüpfung mit einer Inhaltsinformation, die erforderlich ist, den Inhalt zu handhaben, wenn er von der Einrichtung empfangen wird.

6. System nach Anspruch 5, in dem die Verteilung einer Mehrzahl von unterschiedlichen Inhaltstypen von dem System verwaltet wird und ein Packer für jeden Inhaltstyp bereitgestellt wird.

7. System nach Anspruch 5 oder Anspruch 6, in dem die Information, die mit einem Inhalt verknüpft ist, eine Identifikation eines zu verwendenden Installierers aufweist, um den Inhalt auf der Einrichtung zu installieren.

8. System nach einem der vorherigen Ansprüche, das weiterhin ein Verwaltungstool bzw. - werkzeug (210) aufweist für das Bereitstellen einer Schnittstelle, um es einem Benutzer zu ermöglichen, die in der Datenbank gespeicherte hierarchische Struktur zu verwalten.

9. System nach Anspruch 8, in dem die Elemente ein oder mehrere Bereiche beinhalten, wobei jeder Bereich eine logische Gruppierung für Einrichtungen bzw. Geräte darstellt, wobei das Verwaltungstool es ermöglicht, daß Bereiche erzeugt und gelöscht werden, und es ermöglicht, daß Inhaltsidentifizierer mit jedem Bereich verknüpft werden.

Nintendo Exhibit 1003
Part 1 of 2
Page 00604

10. System nach Anspruch 9, in dem das Profil, das von dem Server erzeugt wird, jeden Inhaltsidentifizierer enthält, der mit der Einrichtung verknüpft ist, und alle Inhaltsidentifizierer enthält, die mit einem Bereich verknüpft sind, von dem die Einrichtung in der hierarchischen Struktur abhängt.

11. System nach einem der Ansprüche 8 bis 10, in dem das Verwaltungstool es ermöglicht, daß Personenidentifizierer, die Individuen identifizieren, als Elemente in der hierarchischen Struktur bereitgestellt werden, wobei das Verwaltungstool verwendet werden kann, um innerhalb der hierarchischen Struktur die Einrichtung mit den Individuen, die die Einrichtung besitzen, zu verknüpfen.

12. System nach einem der vorherigen Ansprüche, in dem der Gerätemanager derart angeordnet ist, daß er zu vorbestimmten Zeitintervallen eine Verbindung mit dem Server herstellt, um das Profil abzufragen, wobei der Gerätemanager die Einrichtung identifiziert, für die das Profil erforderlich ist.

13. System nach einem der vorherigen Ansprüche, in dem die Verteilung einer Mehrzahl von unterschiedlichen Inhaltstypen von dem System verwaltet wird und zumindest einer der Typen ein Computerprogramme-Typ ist.

14. System nach einem der vorherigen Ansprüche, in dem die Datenbank eine relationale Datenbank ist.

15. Computerprogrammprodukt, das ein Computerprogramm zur Verfügung stellt, das betreibbar ist, um einen Server (30) zu konfigurieren für die Verwendung in einem System nach einem der vorherigen Ansprüche, wobei das Computerprogramm im Betrieb derart angeordnet ist, daß es veranlaßt, daß der Server die Schritte ausführt:

    Zugreifen auf eine Datenbank, die eine Anzahl von Elementen als eine hierarchische Struktur von Einrichtungen bzw. Geräten, die Inhaltsidentifizierer, die in der Lage sind, mit Elementen in der hierarchischen Struktur verknüpft zu werden, und eines der Elemente, das eine Einrichtung darstellt, zu der Inhalt verteilt werden soll, zur Verfügung stellt, und
    Bezugnehmen (470) auf die hierarchische Struktur in der Datenbank, um ein Profil für die Einrichtung zu erzeugen, wobei das Profil, das eine Anzahl von Inhaltsidentifizierern enthält, Inhalt anzeigt, der zu der Einrichtung bereitgestellt wird, wobei das Profil jeden Inhaltsidentifizierer, der mit dem Element, das die Einrichtung darstellt, verknüpft ist, zusammen mit allen Inhaltsidentifizierern, die mit Elementen in der hierarchischen Struktur verknüpft sind, von denen das Element abhängt, enthält.

16. Computerprogrammprodukt nach Anspruch 15, das weiterhin derart betreibbar ist, daß es den Server konfiguriert, um das Profil zu einem Gerätemanager der Einrichtung zu übertragen (480).

17. Computerprogrammprodukt nach Anspruch 16, wobei das Profil in Antwort auf eine Anfrage nach dem Profil von dem Gerätemanager erzeugt wird.

18. Computerprogrammprodukt nach einem der Ansprüche 15 bis 17, das weiterhin derart betreibbar ist, daß es einen Computer konfiguriert, um eine Schnittstelle bereitzustellen, um es einem Benutzer zu ermöglichen, die hierarchische Struktur, die in der Datenbank gespeichert ist, zu verwalten.

19. Computerprogrammprodukt nach Anspruch 18, in dem die Elemente in der hierarchischen Struktur ein oder mehrere Bereiche beinhalten, wobei jeder Bereich eine logische Gruppierung für Geräte darstellt, wobei das Computerprogramm ermöglicht, daß Bereiche erzeugt und gelöscht werden, und ermöglicht, daß Inhaltsidentifizierer mit jedem Bereich verknüpft werden.

20. Computerprogrammprodukt nach Anspruch 18 oder Anspruch 19, wobei das Computerprogramm es ermöglicht, daß Personenidentifizierer, die Individuen identifizieren, als Elemente in der hierarchischen Struktur bereitgestellt werden, wobei das Computerprogramm verwendet werden kann, um innerhalb der hierarchischen Struktur das Gerät mit dem Individuum, das die Einrichtung besitzt, zu verknüpfen.

21. Computerprogrammprodukt nach einem der Ansprüche 15 bis 20, das weiterhin derart betreibbar ist, daß es einen Computer konfiguriert, um eine Verknüpfung mit einer Inhaltsinformation durchzuführen, die erforderlich ist, um den Inhalt zu handhaben, wenn er von dem Gerät empfangen wird.

22. Computerprogrammprodukt, das ein Computerprogramm bereitstellt, das betreibbar ist, um einen Gerätemanager (200) eines Gerätes bzw. einer Einrichtung (10, 100, 110, 120) für die Verwendung in einem System nach einem der Ansprüche 1 bis 14 zu konfigurieren, wobei das System eine Datenbank (40) hat, die eine Anzahl von Elementen als eine hierarchische Struktur von Geräten, Inhaltsidentifizierer, die mit Elementen in der hierarchischen Struktur verknüpft werden können, und eines der Elemente, das die Einrichtung darstellt, bereitstellt, wobei das Computerprogramm derart angeordnet ist, daß es im Betrieb veranlaßt, daß der Gerätemanager die Schritte durchführt:

Nintendo Exhibit 1003
Part 1 of 2
Page 00605

Empfangen (410) eines Profils von einem Server (30), wobei das Profil erzeugt wurde durch Bezugnehmen auf die hierarchische Struktur in der Datenbank, um ein Profil für die Einrichtung zu erzeugen, wobei das Profil eine Anzahl von Inhaltsidentifizierern enthält, die den Inhalt, der der Einrichtung bereitzustellen ist, anzeigt, wobei das Profil alle Inhaltsidentifizierer, die mit dem Element, das die Einrichtung darstellt, verknüpft sind, zusammen mit allen Inhaltsidentifizierern, die mit Elementen in der hierarchischen Struktur verknüpft sind, von denen das Element abhängt, enthält,
Verwenden der Inhaltsidentifizierer in dem Profil, um zu veranlassen, daß der Inhalt, der von dem Profil angezeigt wird, zu der Einrichtung bzw. zu dem Gerät bereitgestellt wird (430),
Vergleichen (550) mit Empfang eines nachfolgenden Profils von dem Server, der Inhaltsidentifizierer in dem nachfolgenden Profil mit einem Eintrag (560), der den Inhalt identifiziert, der in Übereinstimmung mit einem vorherigen Profil dem Gerät bereitgestellt wurde, um neuen Inhalt, der noch nicht zu der Einrichtung bereitgestellt wurde, und alten Inhalt, der der Einrichtung nicht mehr länger bereitgestellt wird, zu bestimmen und Verwenden der relevanten Inhaltsidentifizierer, um zu veranlassen, daß der neue Inhalt zu der Einrichtung bereitgestellt wird (625), und um zu veranlassen, daß der alte Inhalt entfernt wird (580, 585).

23. Verfahren zum Verwalten der Verteilung von Inhalt zu einem Gerät, das die Schritte aufweist:

Speichern einer Anzahl von Elementen als hierarchische Struktur von Geräten von Inhaltsidentifizierern, die mit Elementen in der hierarchischen Struktur verknüpft werden können, und einem der Elemente, das die Einrichtung bzw. das Gerät darstellt, in einer Datenbank (40),
Bezugnehmen (470) auf die hierarchische Struktur in der Datenbank, um ein Profil für das Gerät zu erzeugen, wobei das Profil eine Anzahl von Inhaltsidentifizierern enthält, die den Inhalt anzeigt, der dem Gerät bereitgestellt werden soll, wobei das Profil alle Inhaltsidentifizierer, die mit dem Element, das das Gerät darstellt, verknüpft sind, zusammen mit allen Inhaltsidentifizierern, die mit Elementen in der hierarchischen Struktur verknüpft sind, von denen das Element abhängt, enthält,
Veranlassen, daß der Inhalt, der von dem Profil angezeigt wird, zu dem Gerät bereitgestellt wird (430) unter Bezug auf die Inhaltsidentifizierer in dem Profil,
Beibehalten eines Eintrages (560), der den Inhalt identifiziert, der Einrichtungen in Übereinstimmung mit dem Profil bereitgestellt wird,
Vergleichen (550) mit Empfang eines nachfolgenden Profils der Inhaltsidentifizierer in dem nachfolgenden Profil mit dem Eintrag, um neuen Inhalt, der noch nicht zu dem Gerät geliefert wurde, und alten Inhalt, der nicht länger zu dem Gerät geliefert wird, zu bestimmen und Verwenden der relevanten Inhaltsidentifizierer, um zu veranlassen, daß der neue Inhalt zu dem Gerät geliefert wird (625) und um zu veranlassen, daß der alte Inhalt entfernt wird (580, 585).

Revendications

1. Système pour gérer une distribution de contenu vers un dispositif (10 ; 100, 110, 120) comprenant :

une base de données (40) pour stocker un certain nombre d'éléments comme une structure hiérarchique de dispositifs, des identificateurs de contenu pouvant être associés à des éléments de la structure hiérarchique, et l'un des éléments représentant le dispositif ;
un serveur (30) pour référencer la structure hiérarchique dans la base de données pour générer un profil pour le dispositif, le profil contenant un certain nombre d'identificateurs de contenu indiquant le contenu à délivrer au dispositif, le profil contenant tous les identificateurs de contenu associés à l'élément représentant le dispositif ainsi que tous les identificateurs de contenu associés à des éléments de la structure hiérarchique dont cet élément dépend ;
un gestionnaire de dispositifs (200) associé au dispositif et configuré pour recevoir le profil à partir du serveur et pour utiliser les identificateurs de contenu du profil pour provoquer la délivrance au dispositif du contenu indiqué par le profil, en conservant un enregistrement identifiant le contenu délivré au dispositif conformément au profil ;
le gestionnaire de dispositifs étant de plus configuré pour comparer, lors de la réception d'un profil suivant à partir du serveur, les identificateurs de contenu du profil suivant avec l'enregistrement pour déterminer le nouveau contenu non encore délivré au dispositif et l'ancien contenu qui n'a plus à être délivré au dispositif, le gestionnaire de dispositifs étant configuré pour utiliser les identificateurs de contenu pertinents pour provoquer la délivrance du nouveau contenu au dispositif et l'élimination de l'ancien contenu.

2. Système selon la revendication 1, dans lequel chaque identificateur de contenu fournit un nom pour

Nintendo Exhibit 1003
Part 1 of 2
Page 00606

le contenu correspondant et un indicateur d'emplacement indentifiant un emplacement à partir duquel ce contenu peut être obtenu.

3. Système selon la revendication 2, dans lequel la distribution d'une pluralité de différents types de contenus est gérée par le système et l'identificateur de contenu indentifie de plus le type du contenu correspondant.

4. Système selon les revendications 2 ou 3, dans lequel le contenu est stocké sur des serveurs (250, 260) contactables par Internet et dans lequel l'indicateur d'emplacement est une adresse URL.

5. Système selon l'une quelconque des revendications précédentes, comprenant de plus un certain nombre d'empaqueteurs (810) à associer à une information de contenu nécessaire à la manipulation du contenu quand il est reçu par le dispositif.

6. Système selon la revendication 5, dans lequel la distribution d'une pluralité de différents types de contenus est gérée par le système et un empaqueteur est fourni pour chaque type de contenu.

7. Système selon les revendications 5 ou 6, dans lequel l'information associée à un contenu comprend une identification d'installateur à utiliser pour installer le contenu sur le dispositif.

8. Système selon l'une quelconque des revendications précédentes, comprenant de plus un outil de gestion (210) pour délivrer une interface autorisant un utilisateur à gérér la structure hiérarchique stockée dans la base de données.

9. Système selon la revendication 8, dans lequel lesdits éléments comprennent une ou plusieurs sections, chaque section représentant un groupement logique de dispositifs, l'outil de gestion permettant la création et la destruction de sections et permettant l'association des identificateurs de contenu à chaque section.

10. Système selon la revendication 9, dans lequel le profil généré par le serveur contient tous les identificateurs de contenu associés au dispositif et tous les identificateurs de contenu associés à la section dont dépend le dispositif dans la structure hiérarchique.

11. Système selon l'une quelconque des revendications 8 à 10, dans lequel l'outil de gestion permet la délivrance, comme éléments de la structure hiérarchique, d'identificateurs de personnes identifiant des individus, identificateurs grâce auxquels l'outil de gestion peut être utilisé pour associer, à l'intérieur de la structure hiérarchique, le dispositif à l'individu possédant ce dispositif.

12. Système selon l'une quelconque des revendications précédentes, dans lequel le gestionnaire de dispositifs est configuré pour réaliser une connexion au serveur, à des intervalles prédéterminés, de manière à demander le profil, le gestionnaire de dispositifs identifiant le dispositif pour lequel le profil est demandé.

13. Système selon l'une quelconque des revendications précédentes, dans lequel la distribution d'une pluralité de différents types de contenus est gérée par le système et dans lequel au moins un desdits types est un programme d'ordinateur.

14. Système selon l'une quelconque des revendications précédentes, dans lequel la base de données est une base de données relationnelle.

15. Produit de programme d'ordinateur fournissant un programme d'ordinateur utilisable pour configurer un serveur (30) pour une utilisation dans un système selon l'une quelconque des revendications précédentes, le programme d'ordinateur étant configuré en fonctionnement pour provoquer l'exécution par le serveur des étapes consistant à :

accéder à une base de données fournissant un certain nombre d'éléments comme une structure hiérarchique de dispositifs, des identificateurs de contenu pouvant être associés à des éléments de la structure hiérarchique, et l'un des éléments représentant un dispositif auquel le contenu doit être distribué ; et
référencer (470) la structure hiérarchique dans la base de données pour générer un profil pour le dispositif, le profil contenant un certain nombre d'identificateurs de contenu indiquant le contenu à délivrer au dispositif, le profil contenant tous les identificateurs de contenu associés à l'élément représentant le dispositif ainsi que tous les identificateurs de contenu associés à des éléments de la structure hiérarchique dont cet élément dépend.

16. Produit de programme d'ordinateur selon la revendication 15, utilisable de plus pour configurer le serveur afin de transmettre (480) le profil à un gestionnaire de dispositifs du dispositif.

17. Produit de programme d'ordinateur selon la revendication 16, dans lequel le profil est généré en réponse à une demande du profil provenant du gestionnaire de dispositifs.

18. Produit de programme d'ordinateur selon l'une

Nintendo Exhibit 1003
Part 1 of 2
Page 00607

quelconque des revendications 15 à 17, utilisable de plus pour configurer un ordinateur pour délivrer une interface autorisant un utilisateur à gérér la structure hiérarchique stockée dans la base de données.

19. Produit de programme d'ordinateur selon la revendication 18, dans lequel les éléments de la structure hiérarchique comprennent une ou plusieurs sections, chaque section représentant un groupement logique de dispositifs, le programme d'ordinateur permettant la création et la destruction de sections et permettant l'association d'identificateurs de contenu à chaque section.

20. Produit de programme d'ordinateur selon les revendications 18 ou 19, dans lequel le programme d'ordinateur permet la délivrance, comme éléments de la structure hiérarchique, d'identificateurs de personnes identifiant des individus, identificateurs grâce auxquels le programme d'ordinateur peut être utilisé pour associer, à l'intérieur de la structure hiérarchique, le dispositif à l'individu possédant ce dispositif.

21. Produit de programme d'ordinateur selon l'une quelconque des revendications 15 à 20, utilisable de plus pour configurer un ordinateur afin d'associer une information de contenu nécessaire à la manipulation du contenu quand il est reçu par le dispositif.

22. Produit de programme d'ordinateur fournissant un programme d'ordinateur utilisable pour configurer un gestionnaire de dispositifs (200) d'un dispositif (10 ; 100, 110, 120) pour une utilisation dans un système selon l'une quelconque des revendications 1 à 14, le système possédant une base de données (40) fournissant un certain nombre d'éléments comme une structure hiérarchique de dispositifs, des identificateurs de contenu pouvant être associés à des éléments de la structure hiérarchique, et l'un des éléments représentant le dispositif, le programme d'ordinateur étant configuré en fonctionnement pour provoquer l'exécution par le gestionnaire de dispositifs des étapes consistant à :

recevoir (410) un profil de serveur (30), le profil ayant été généré en référençant la structure hiérarchique dans la base de données afin de générer un profil pour le dispositif, le profil contenant un certain nombre d'identificateurs de contenu indiquant le contenu à délivrer au dispositif, le profil contenant tous les identificateurs de contenu associés à l'élément représentant le dispositif ainsi que tous les identificateurs de contenu associés à des éléments de la structure hiérarchique dont cet élément dépend ;
utiliser les identificateurs de contenu du profil pour provoquer la délivrance (430) au dispositif du contenu indiqué par le profil ;
comparer (550), lors de la réception d'un profil suivant à partir du serveur, les identificateurs de contenu du profil suivant avec un enregistrement (560) identifiant le contenu délivré au dispositif conformément à un profil précédent pour déterminer le nouveau contenu non encore délivré au dispositif et l'ancien contenu qui n'a plus à être délivré au dispositif, et utiliser les identificateurs de contenu pertinents pour provoquer la délivrance (625) du nouveau contenu au dispositif et l'élimination de l'ancien contenu (580, 585).

23. Procédé de gestion d'une distribution de contenu à un dispositif, comprenant les étapes consistant à :

stocker dans une base de données (40) un certain nombre d'éléments comme une structure hiérarchique de dispositifs, des identificateurs de contenu pouvant être associés à des éléments de la structure hiérarchique, et l'un des éléments représentant le dispositif ;
référencer (470) la structure hiérarchique dans la base de données afin de générer un profil pour le dispositif, le profil contenant un certain nombre d'identificateurs de contenu indiquant le contenu à délivrer au dispositif, le profil contenant tous les identificateurs de contenu associés à l'élément représentant le dispositif ainsi que tous les identificateurs de contenu associés à des éléments de la structure hiérarchique dont cet élément dépend ;
en se référant aux identificateurs de contenu du profil, provoquer la délivrance (430) au dispositif du contenu indiqué par le profil ;
tenir à jour un enregistrement (560) identifiant le contenu délivré au dispositif conformément au profil ;
comparer (550), lors de la réception d'un profil suivant, les identificateurs de contenu du profil suivant avec l'enregistrement pour déterminer le nouveau contenu non encore délivré au dispositif et l'ancien contenu qui n'a plus à être délivré au dispositif, et utiliser les identificateurs de contenu pertinents pour provoquer la délivrance (625) du nouveau contenu au dispositif et l'élimination de l'ancien contenu (580, 585).

Nintendo Exhibit 1003
Part 1 of 2
Page 00608

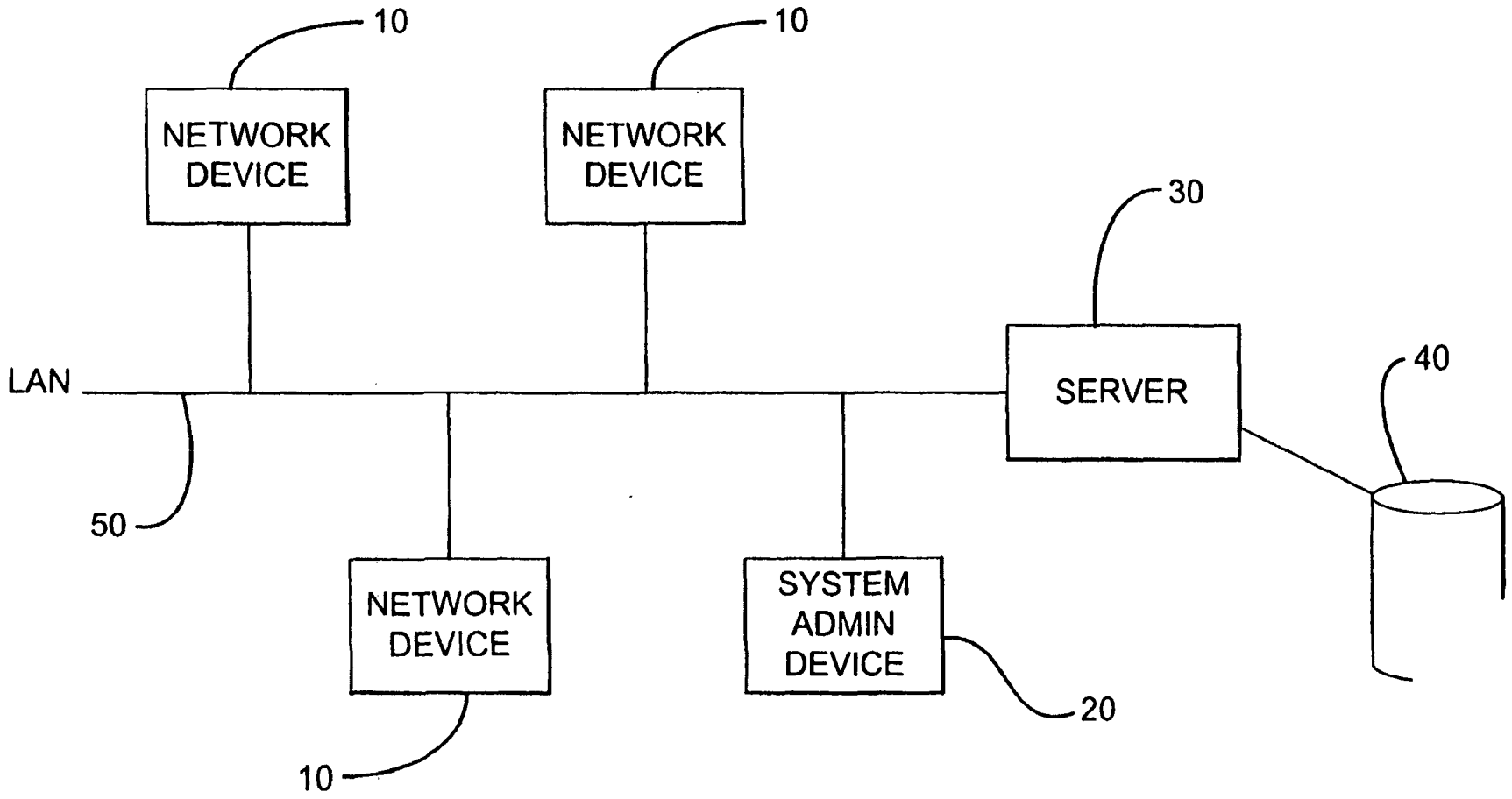
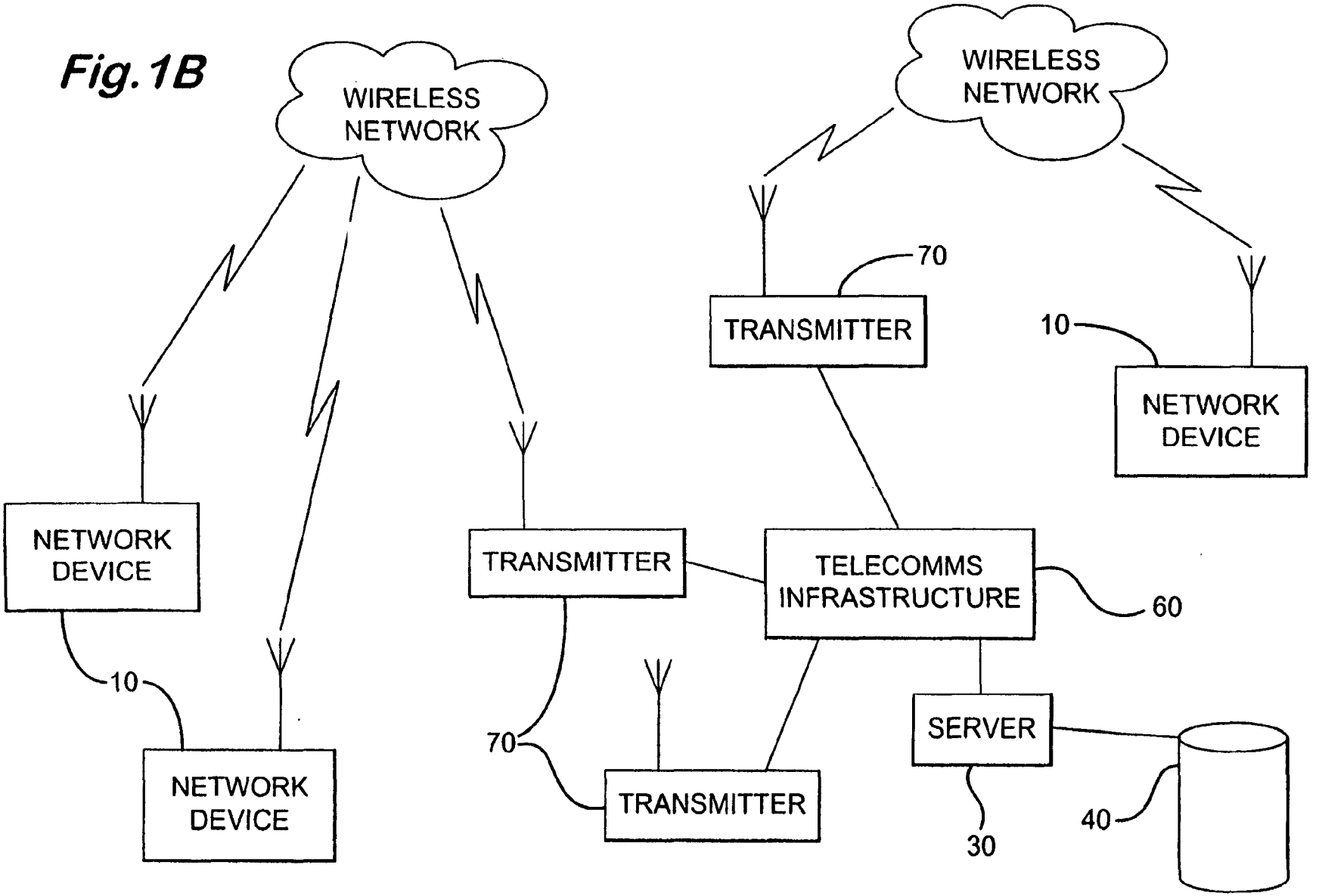


Fig. 1A

EP 1 185 923 B1

Fig. 1B



EP 1 185 923 B1

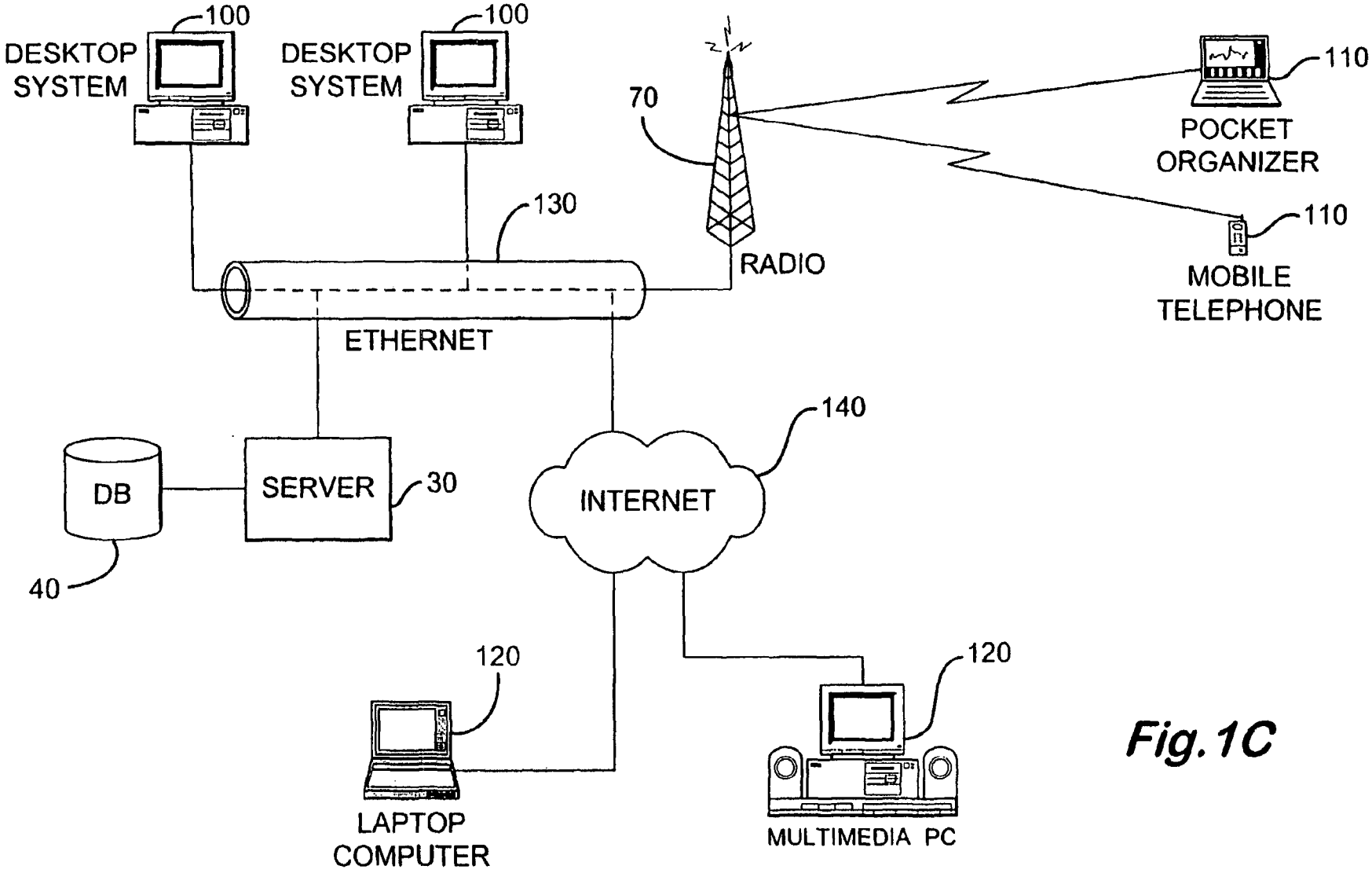


Fig. 1C

EP 1 185 923 B1

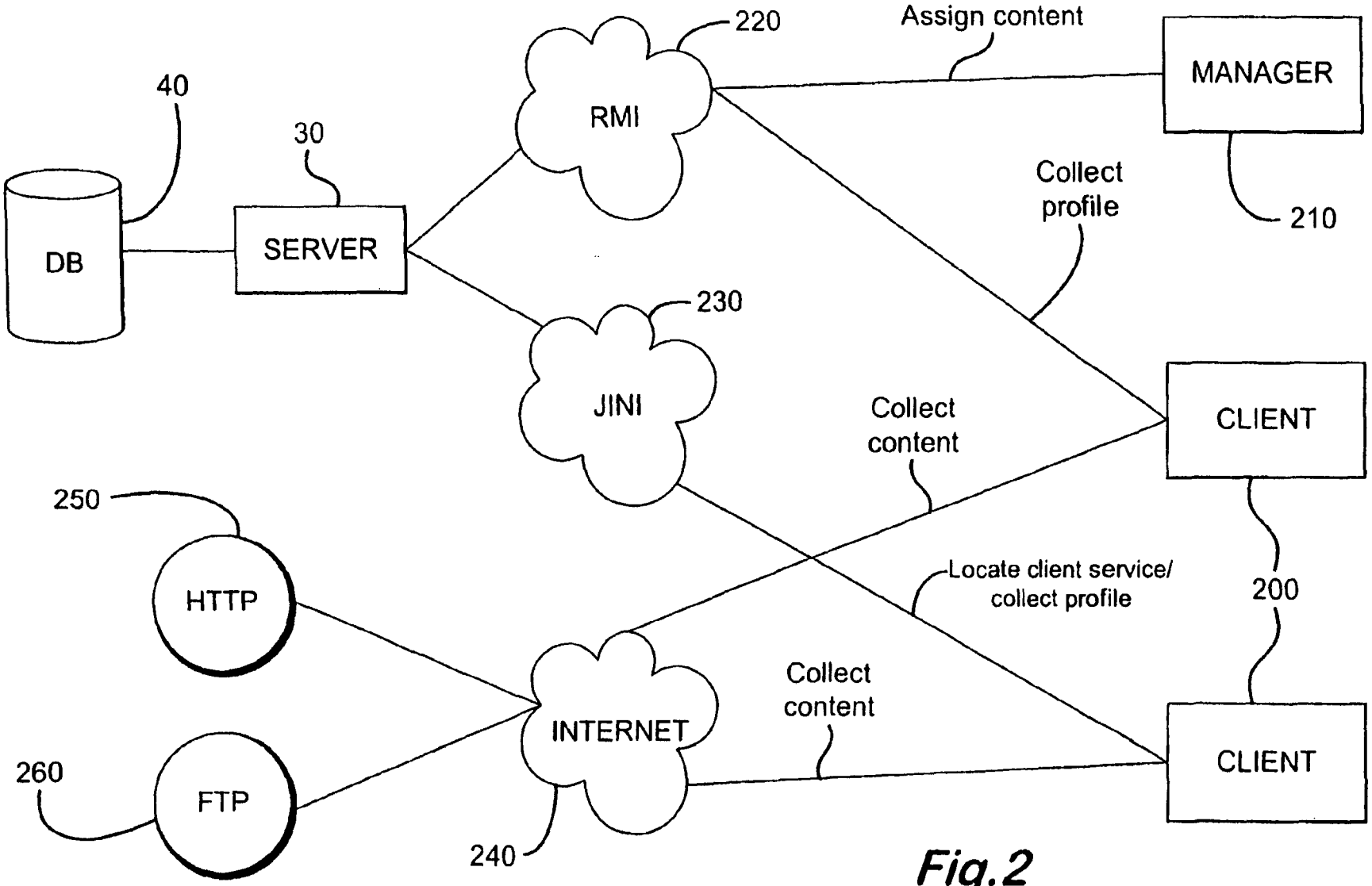


Fig.2

EP 1 185 923 B1

Fig.3

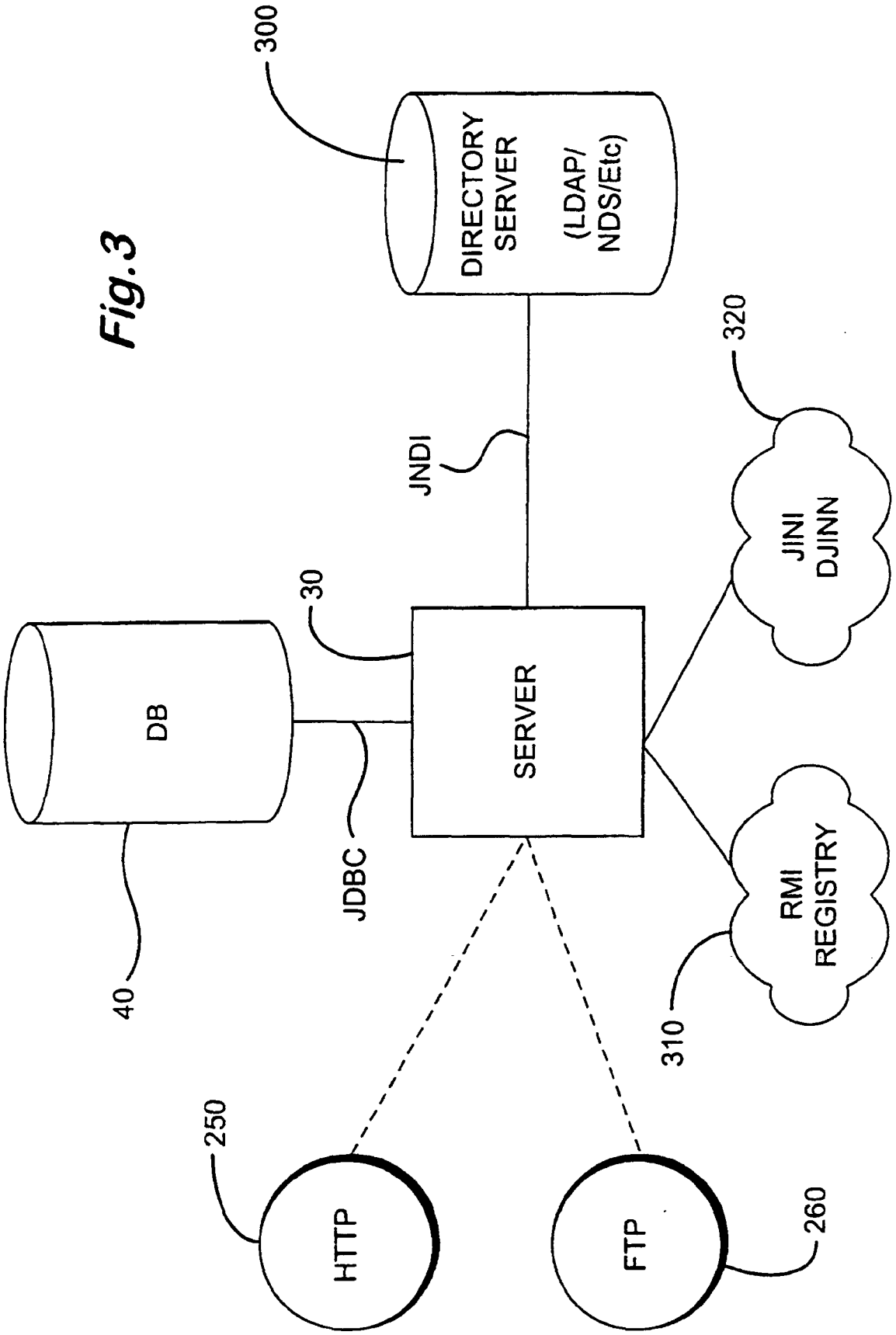
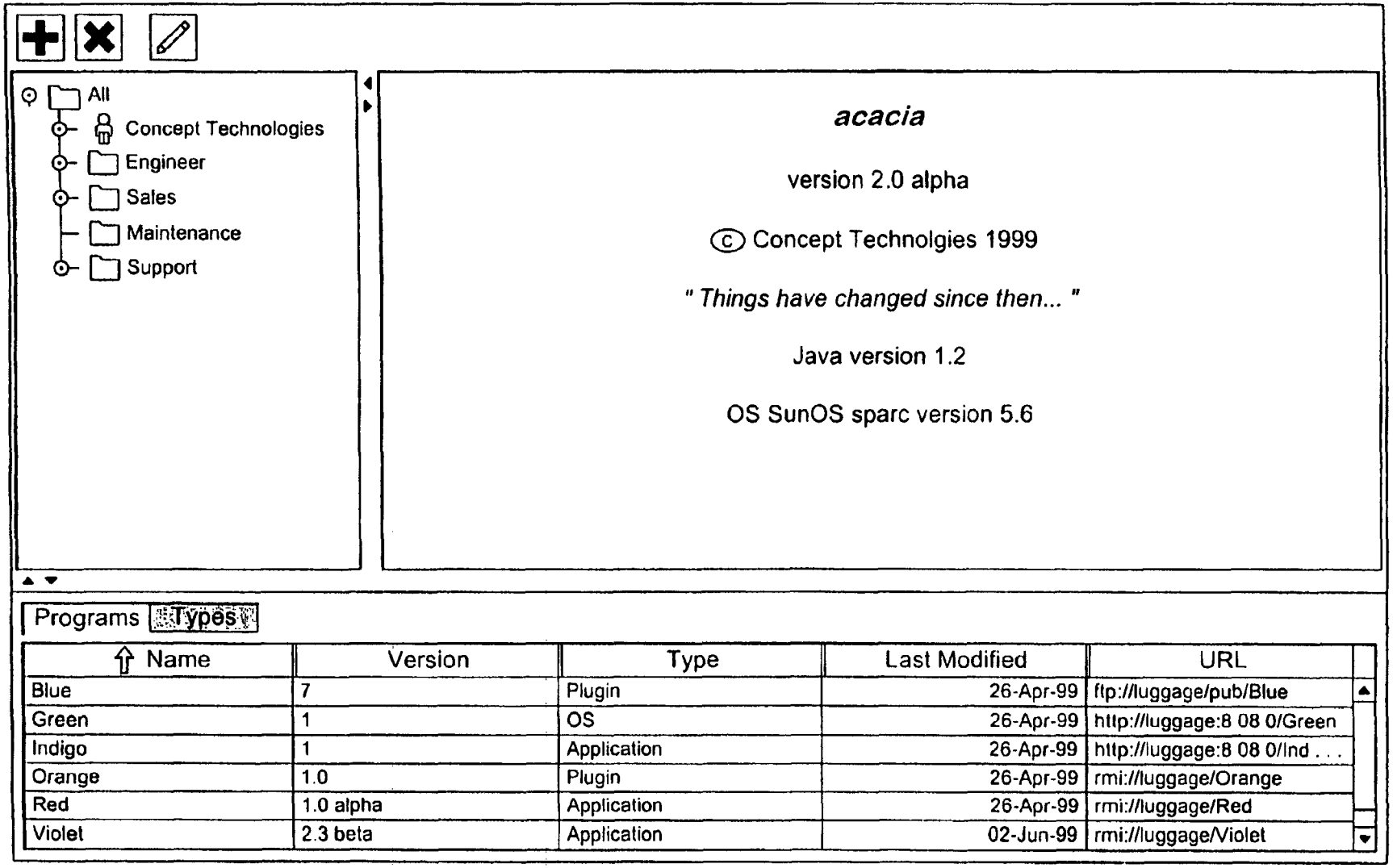

300
DIRECTORY SERVER
(LDAP/ NDS/Etc)
JNDI
320
JINI DJINN
30
SERVER
DB
JDBC
40
RMI REGISTRY
310
250
HTTP
FTP
260

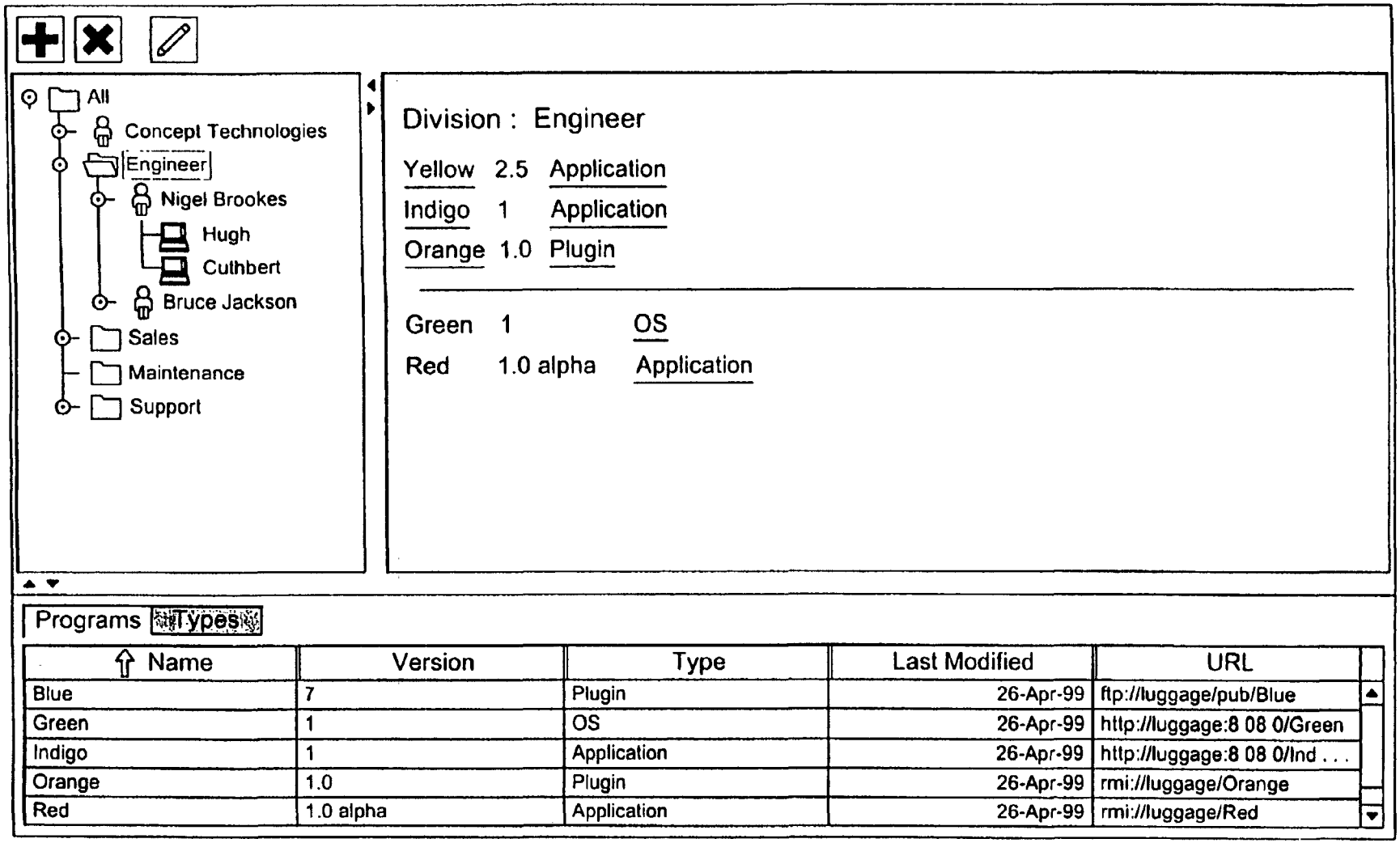
Fig.4



Name	Version	Type	Last Modified	URL
Blue	7	Plugin	26-Apr-99	ftp://luggage/pub/Blue
Green	1	OS	26-Apr-99	http://luggage:8 08 0/Green
Indigo	1	Application	26-Apr-99	http://luggage:8 08 0/Ind . . .
Orange	1.0	Plugin	26-Apr-99	rmi://luggage/Orange
Red	1.0 alpha	Application	26-Apr-99	rmi://luggage/Red
Violet	2.3 beta	Application	02-Jun-99	rmi://luggage/Violet

EP 1 185 923 B1

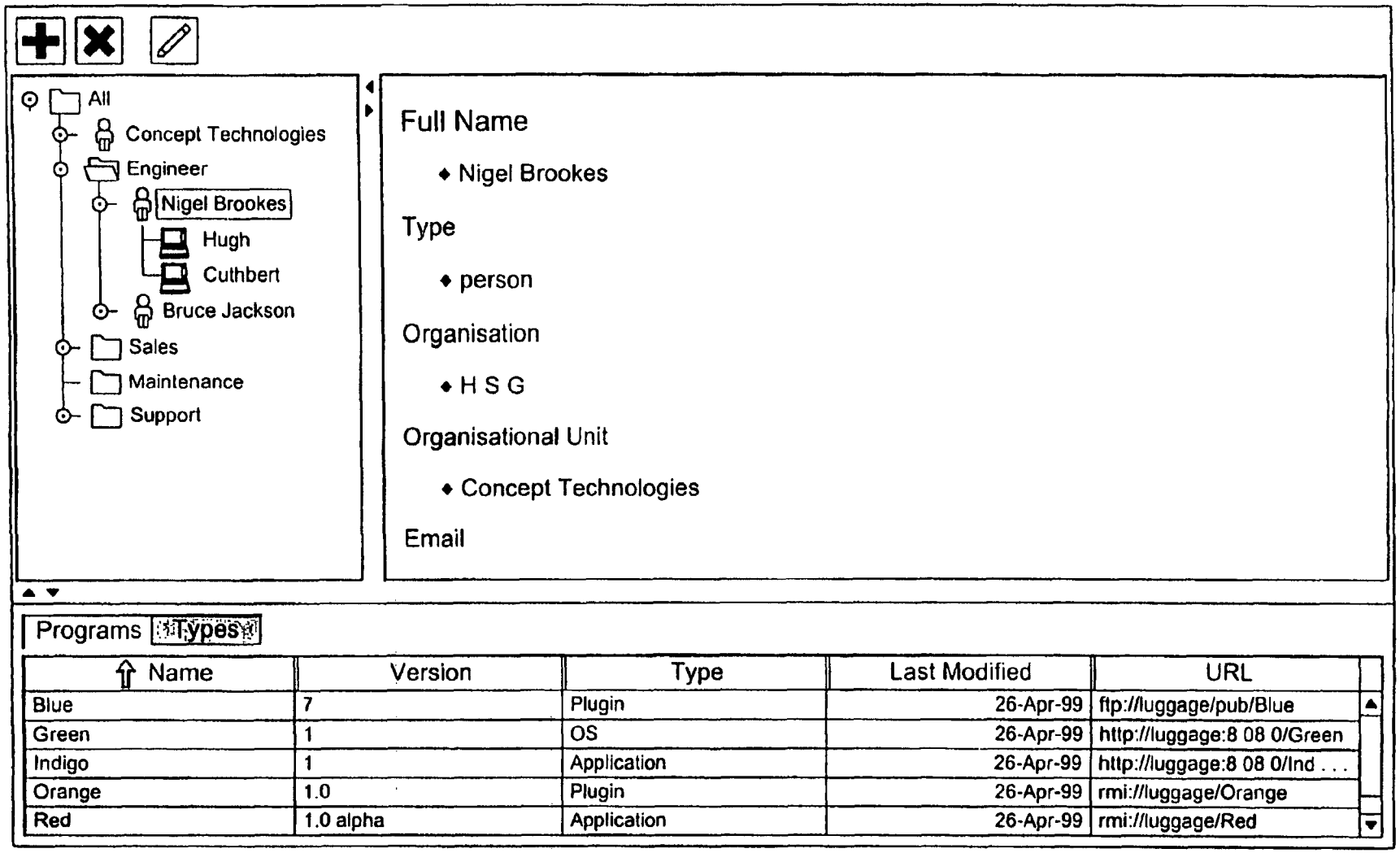
Fig.5



Name	Version	Type	Last Modified	URL
Blue	7	Plugin	26-Apr-99	ftp://luggage/pub/Blue
Green	1	OS	26-Apr-99	http://luggage:8 08 0/Green
Indigo	1	Application	26-Apr-99	http://luggage:8 08 0/Ind . . .
Orange	1.0	Plugin	26-Apr-99	rmi://luggage/Orange
Red	1.0 alpha	Application	26-Apr-99	rmi://luggage/Red

EP 1 185 923 B1

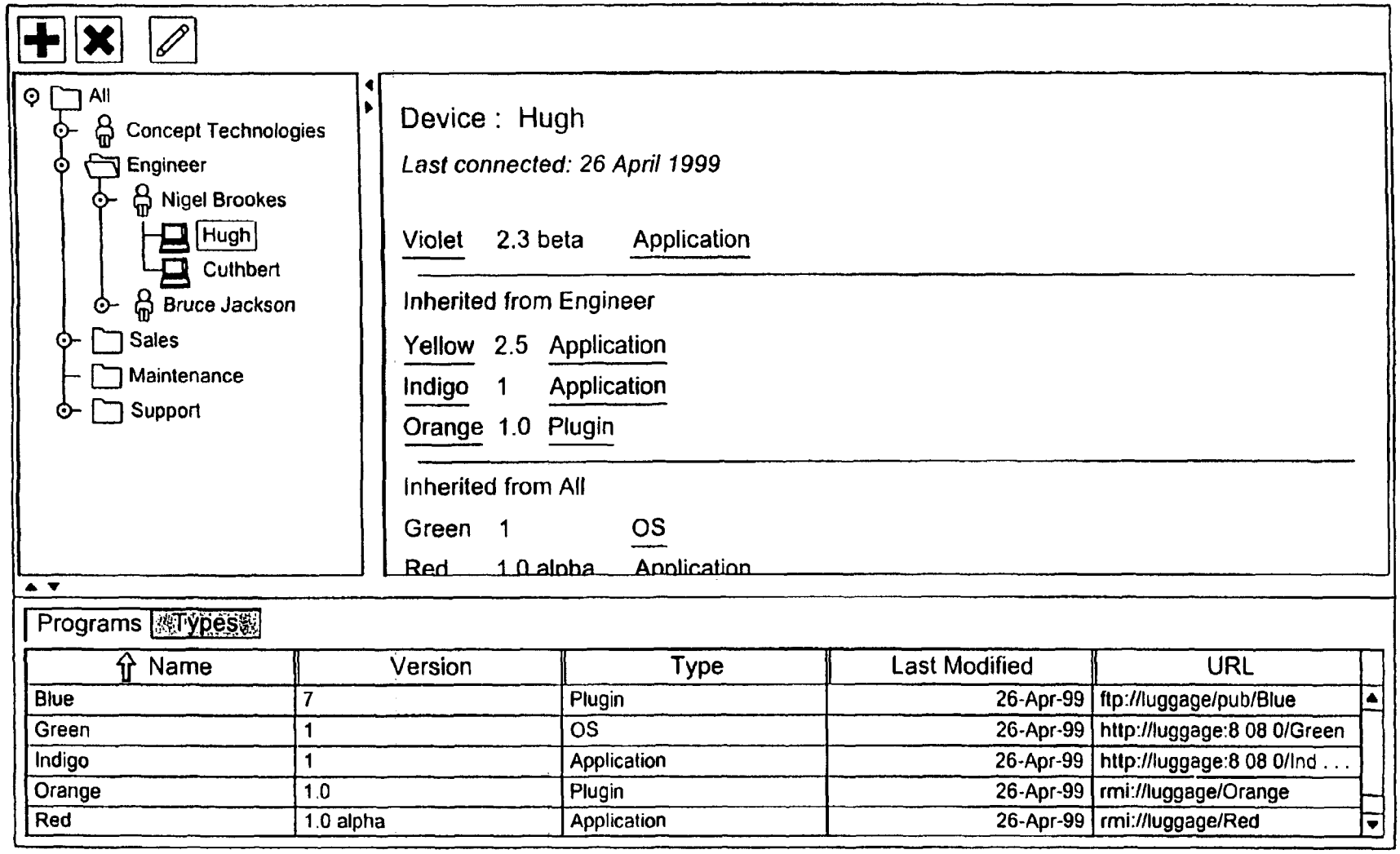
Fig.6



Name	Version	Type	Last Modified	URL
Blue	7	Plugin	26-Apr-99	ftp://luggage/pub/Blue
Green	1	OS	26-Apr-99	http://luggage:8 08 0/Green
Indigo	1	Application	26-Apr-99	http://luggage:8 08 0/Ind . . .
Orange	1.0	Plugin	26-Apr-99	rmi://luggage/Orange
Red	1.0 alpha	Application	26-Apr-99	rmi://luggage/Red

EP 1 185 923 B1

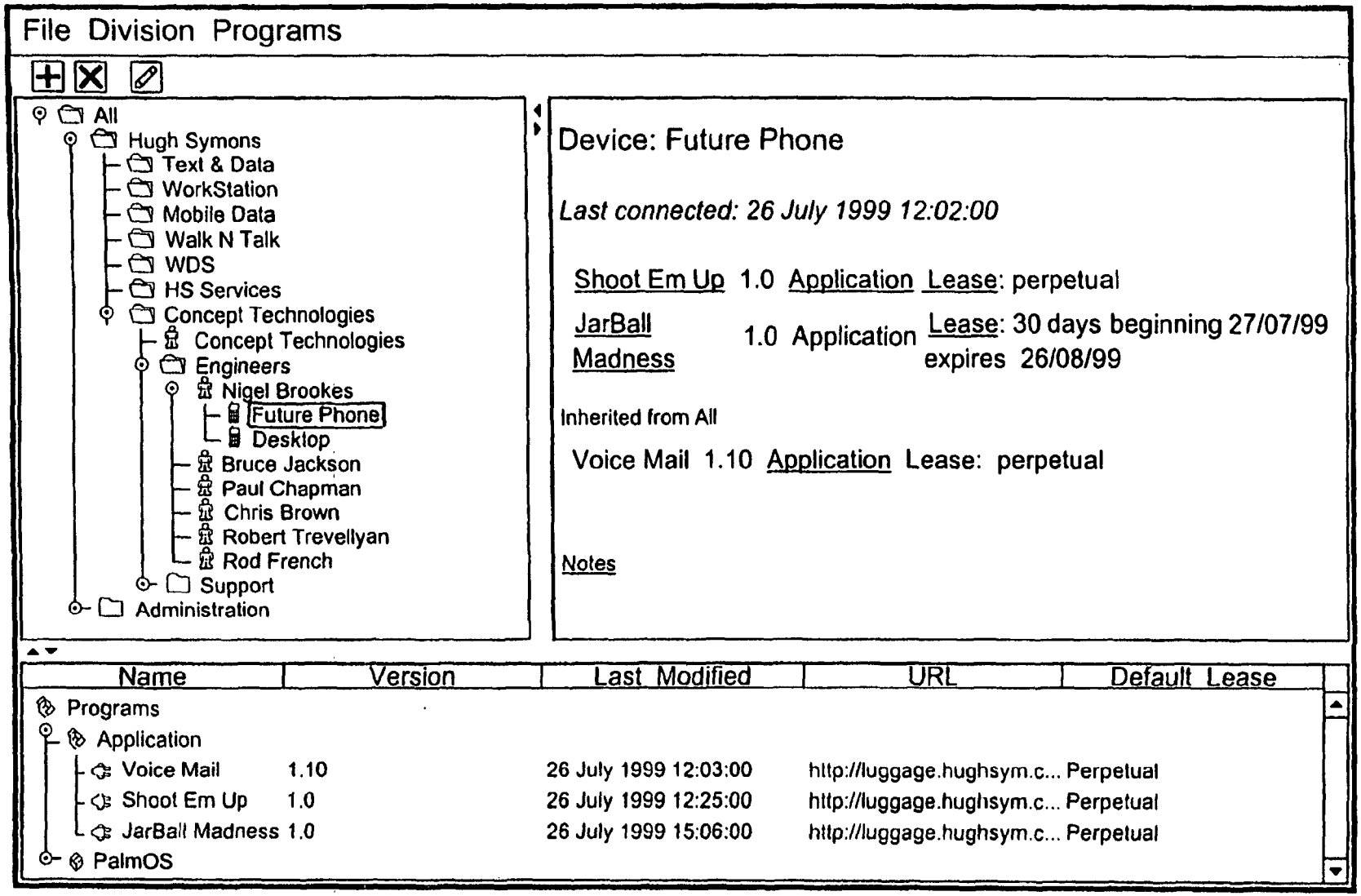
Fig. 7



Name	Version	Type	Last Modified	URL
Blue	7	Plugin	26-Apr-99	ftp://luggage/pub/Blue
Green	1	OS	26-Apr-99	http://luggage:8 08 0/Green
Indigo	1	Application	26-Apr-99	http://luggage:8 08 0/Ind . . .
Orange	1.0	Plugin	26-Apr-99	rmi://luggage/Orange
Red	1.0 alpha	Application	26-Apr-99	rmi://luggage/Red

EP 1 185 923 B1

Fig.8



EP 1 185 923 B1

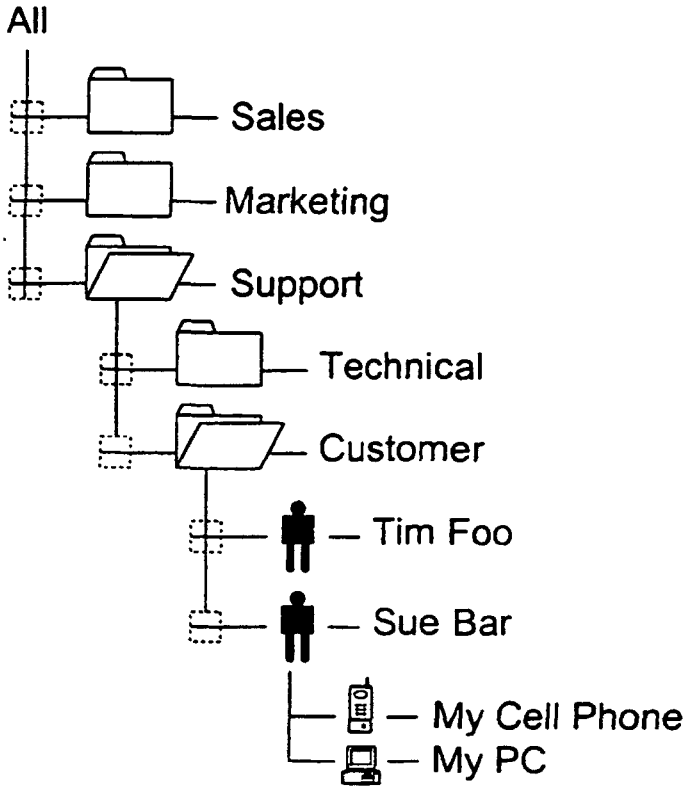

All
Sales
Marketing
Support
Technical
Customer
Tim Foo
Sue Bar
My Cell Phone
My PC

Fig.9

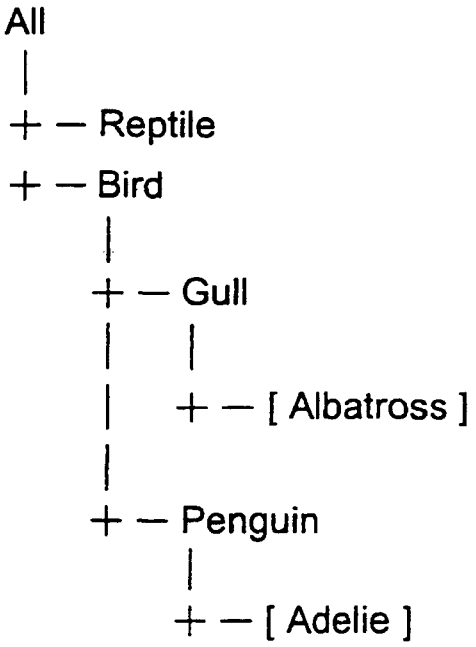

All
+ — Reptile
+ — Bird
+ — Gull
+ — [Albatross]
+ — Penguin
+ — [Adelie]

Fig.10

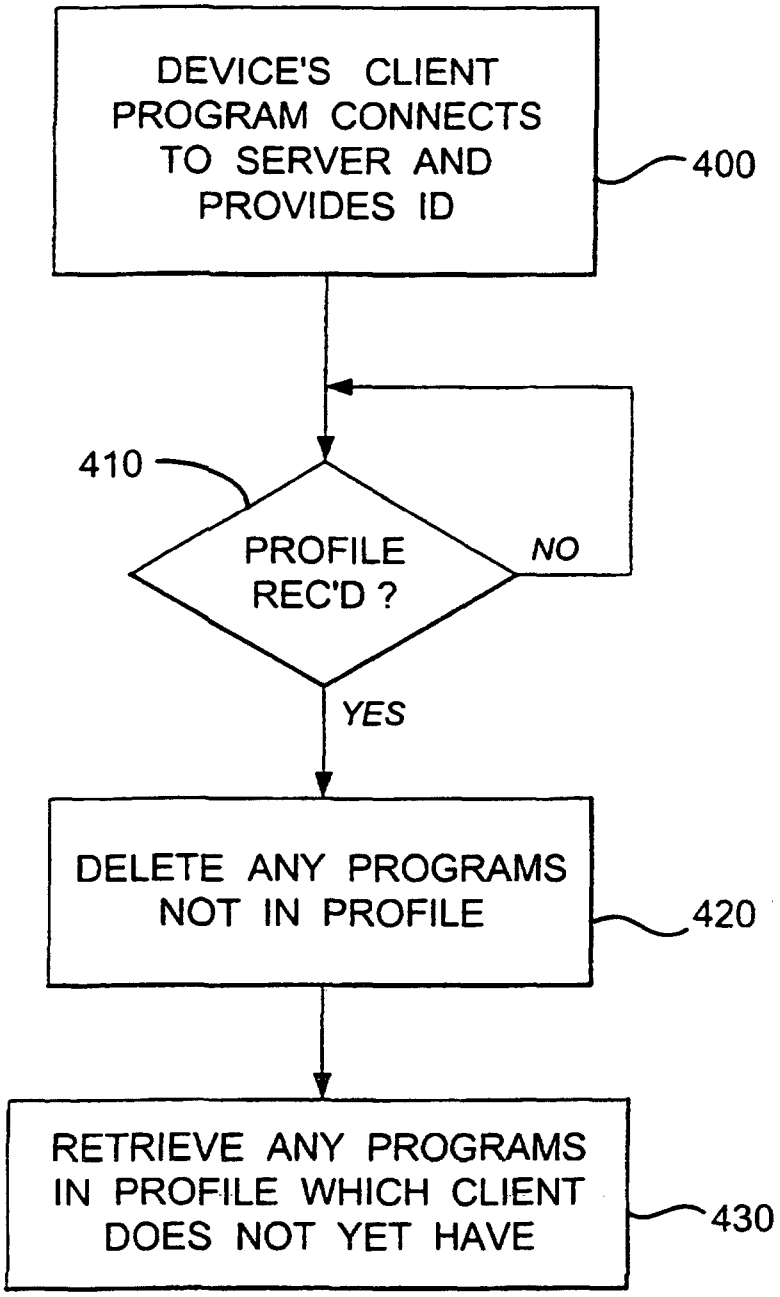

DEVICE'S CLIENT PROGRAM CONNECTS TO SERVER AND PROVIDES ID
400
410
PROFILE REC'D ?
NO
YES
DELETE ANY PROGRAMS NOT IN PROFILE
420
RETRIEVE ANY PROGRAMS IN PROFILE WHICH CLIENT DOES NOT YET HAVE
430

Fig. 11

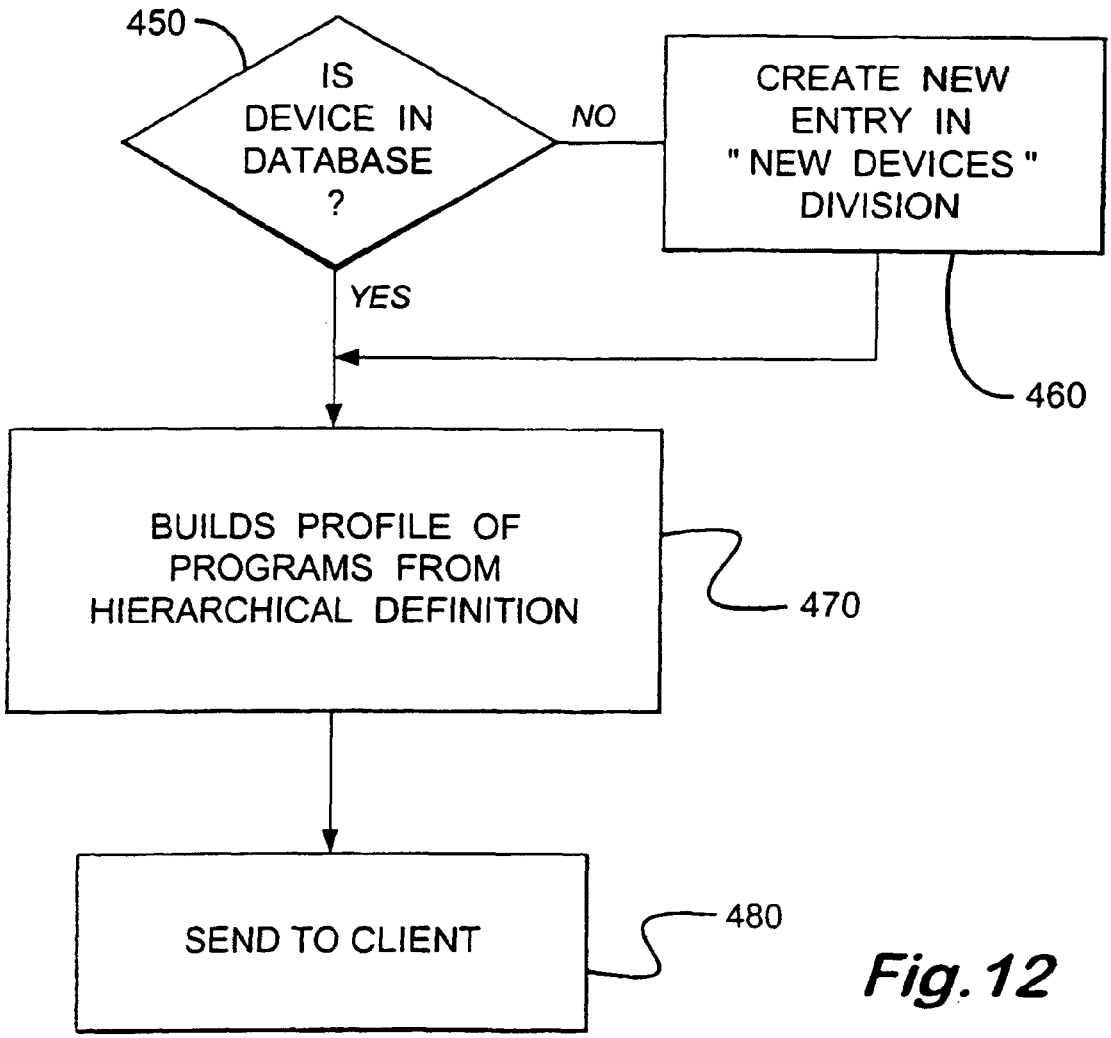

450
IS DEVICE IN DATABASE ?
NO
CREATE NEW ENTRY IN " NEW DEVICES " DIVISION
YES
460
BUILDS PROFILE OF PROGRAMS FROM HIERARCHICAL DEFINITION
470
SEND TO CLIENT
480

Fig.12

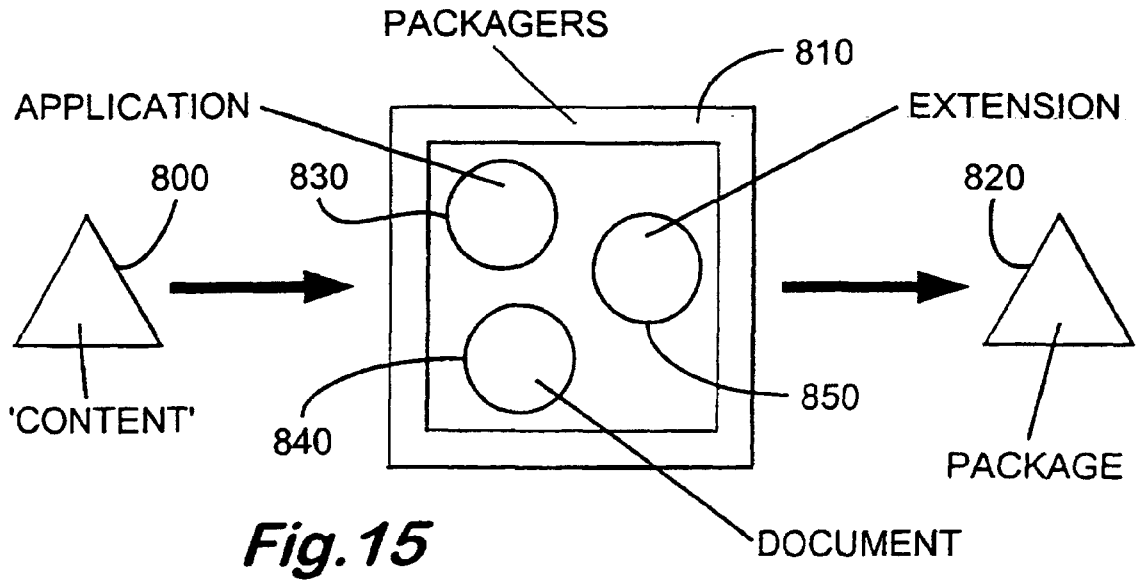

PACKAGERS
810
APPLICATION
EXTENSION
800
830
820
'CONTENT'
840
850
PACKAGE
DOCUMENT

Fig.15

Fig.13A

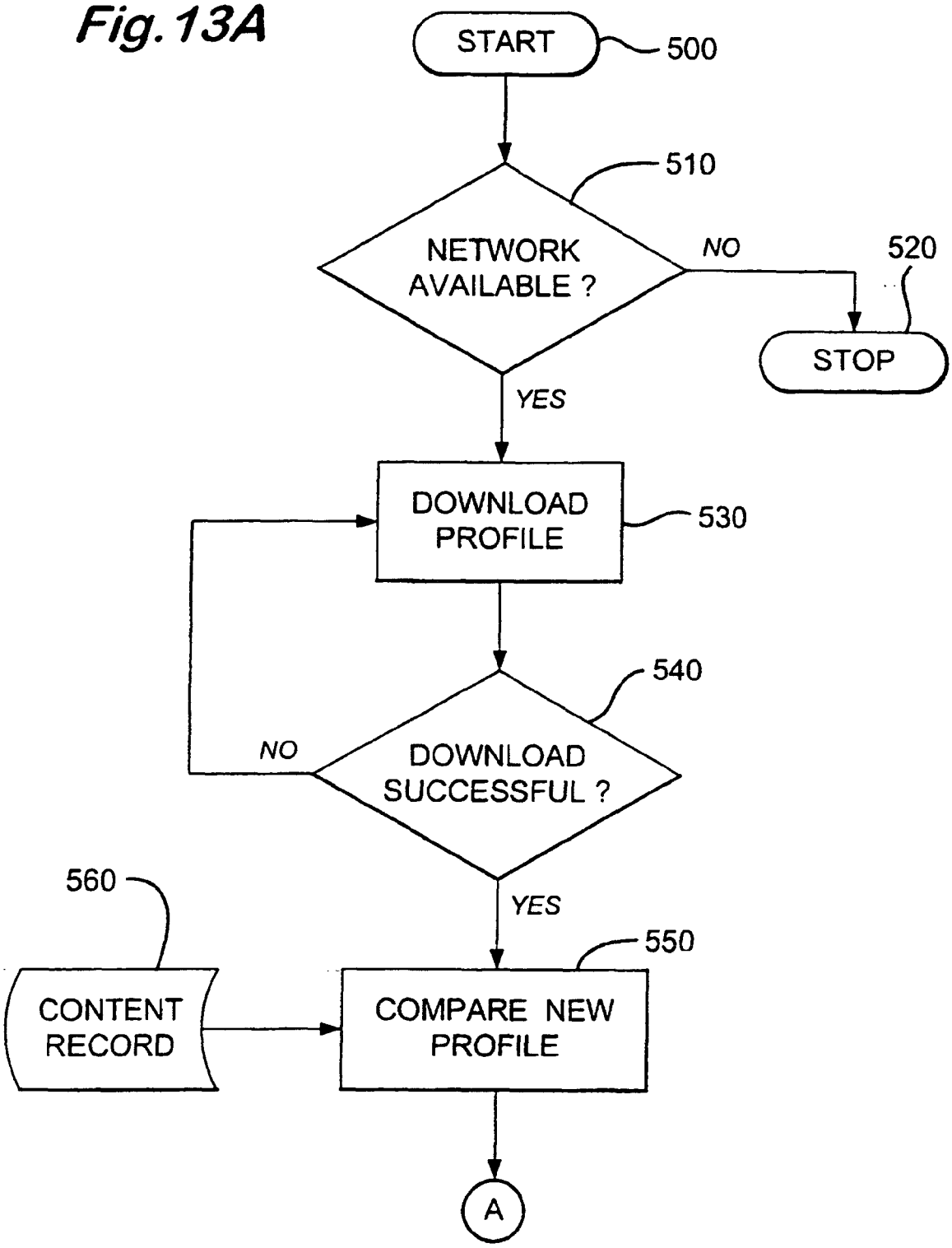
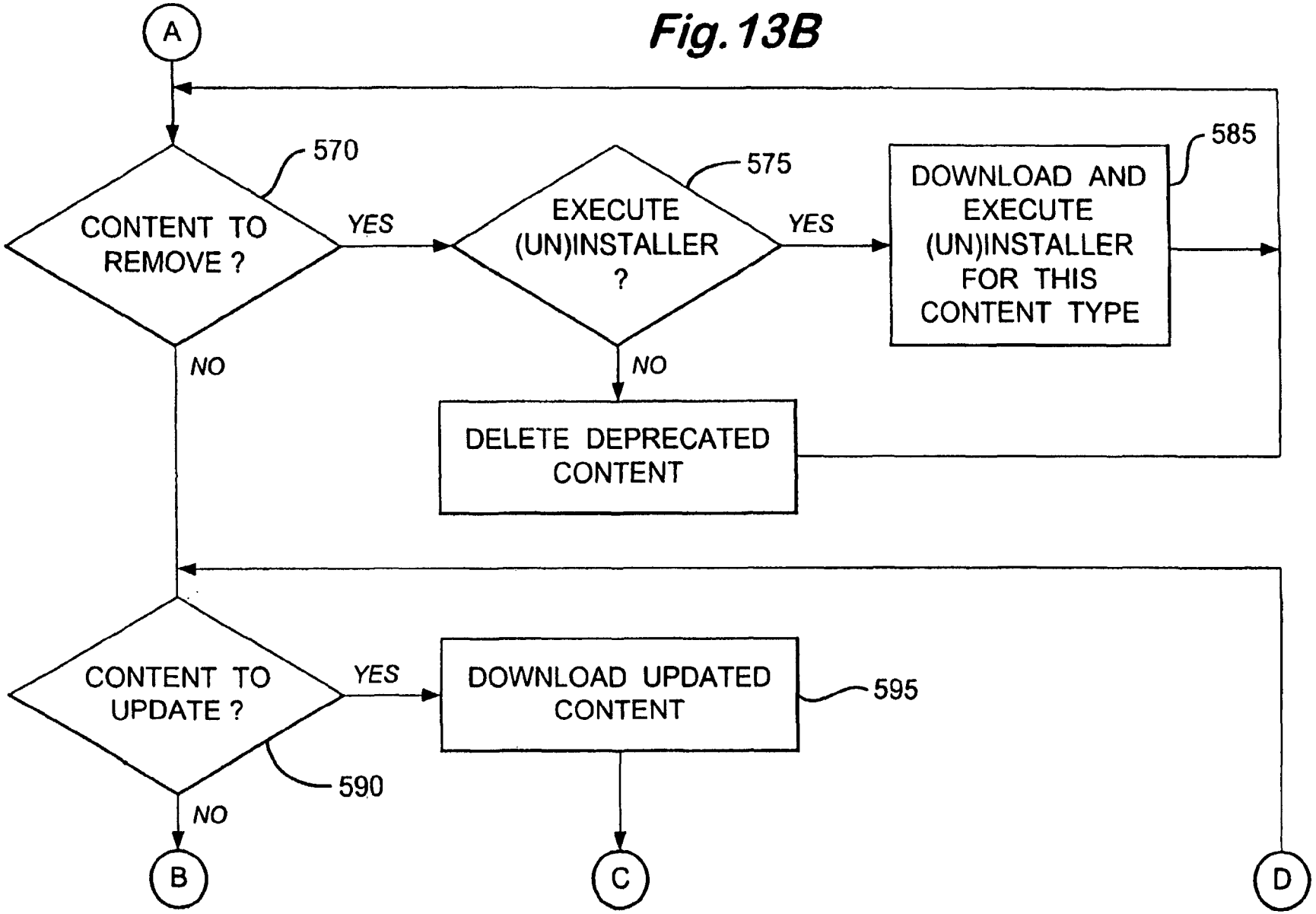

START
500
510
NETWORK AVAILABLE ?
NO
520
STOP
YES
DOWNLOAD PROFILE
530
540
NO
DOWNLOAD SUCCESSFUL ?
YES
560
CONTENT RECORD
550
COMPARE NEW PROFILE
A

Fig.13B



EP 1 185 923 B1

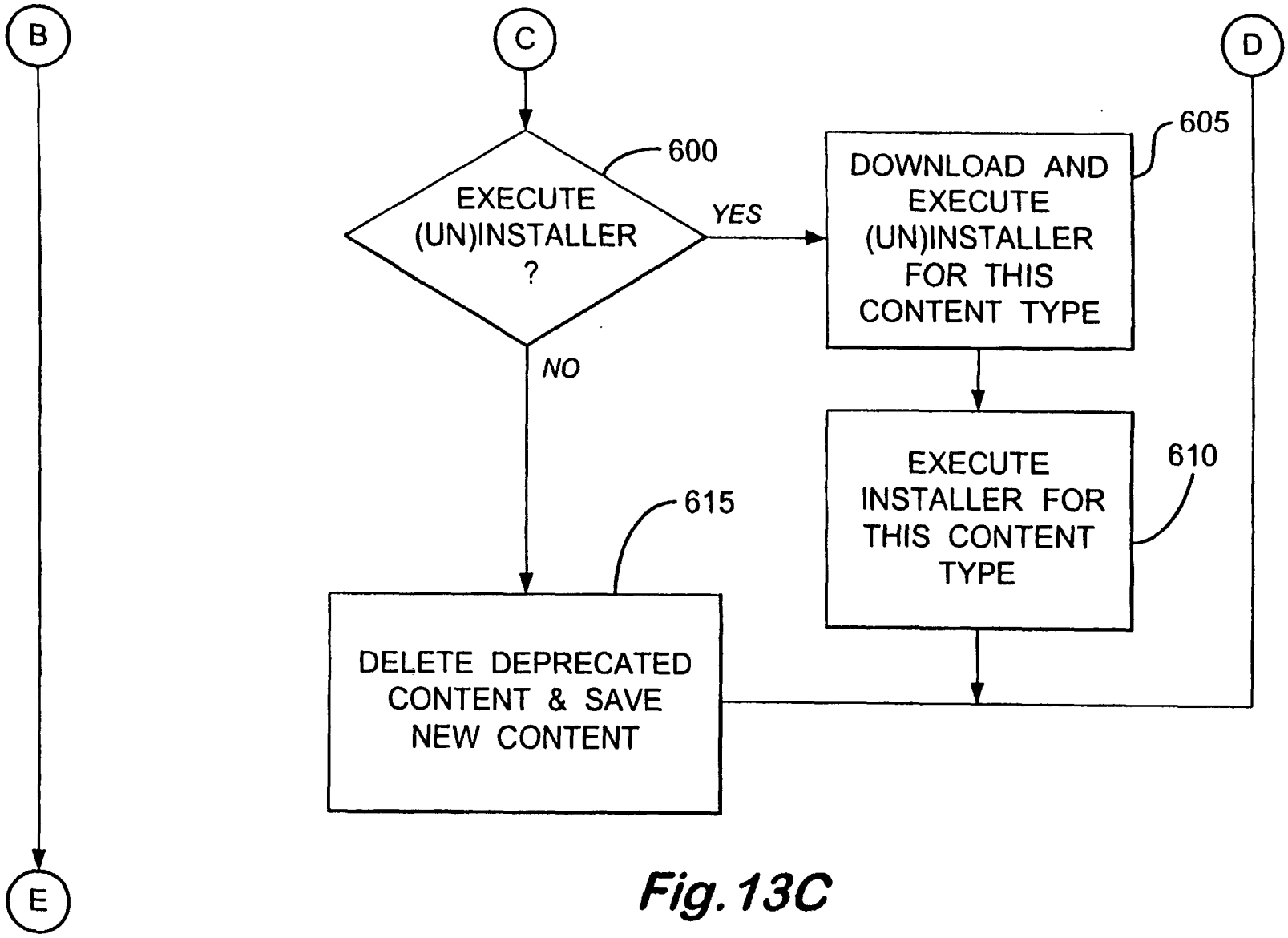


Fig. 13C

EP 1 185 923 B1

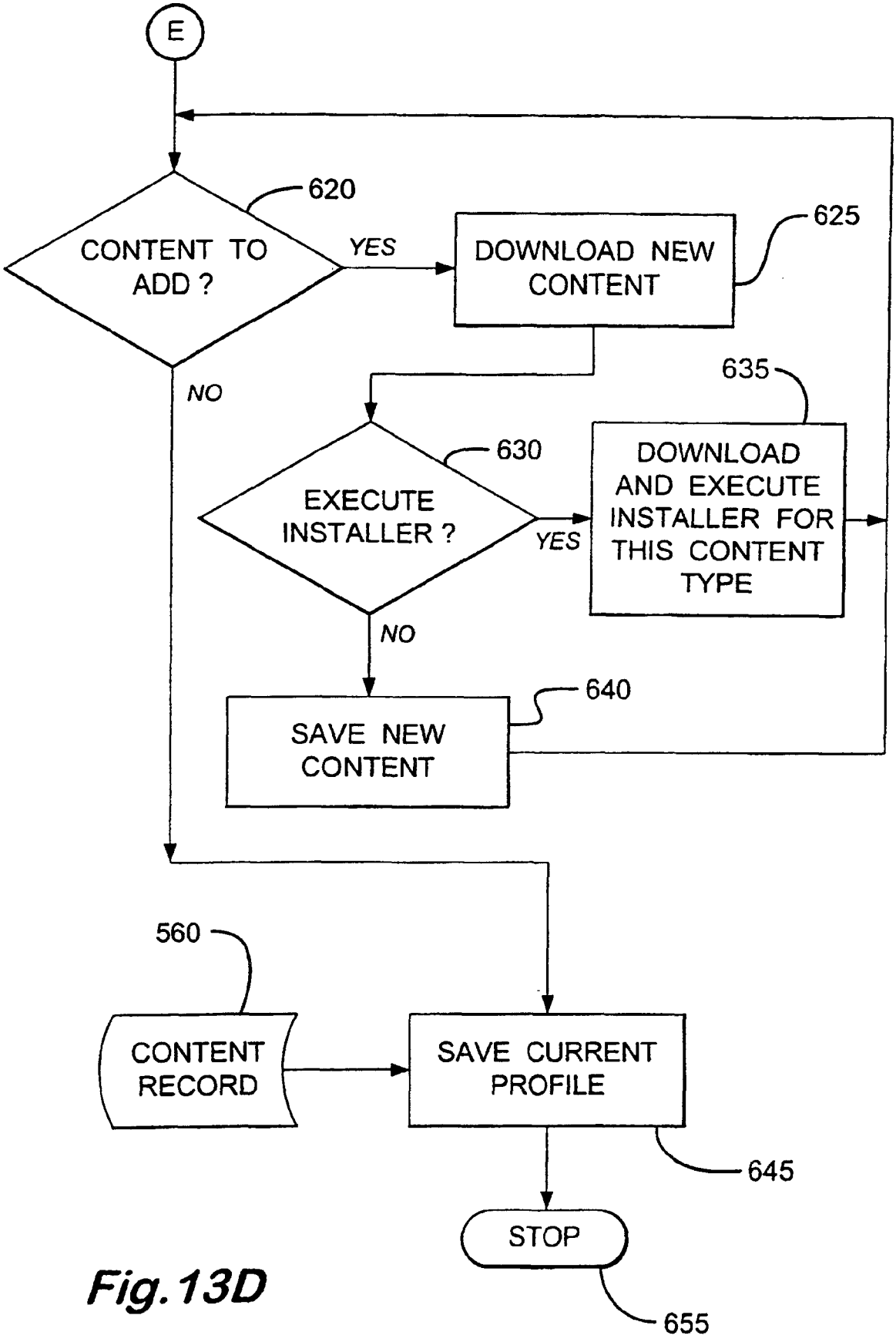

E
620
CONTENT TO ADD ?
YES
DOWNLOAD NEW CONTENT
625
NO
635
630
EXECUTE INSTALLER ?
YES
DOWNLOAD AND EXECUTE INSTALLER FOR THIS CONTENT TYPE
NO
640
SAVE NEW CONTENT
560
CONTENT RECORD
SAVE CURRENT PROFILE
645
STOP
655

Fig. 13D

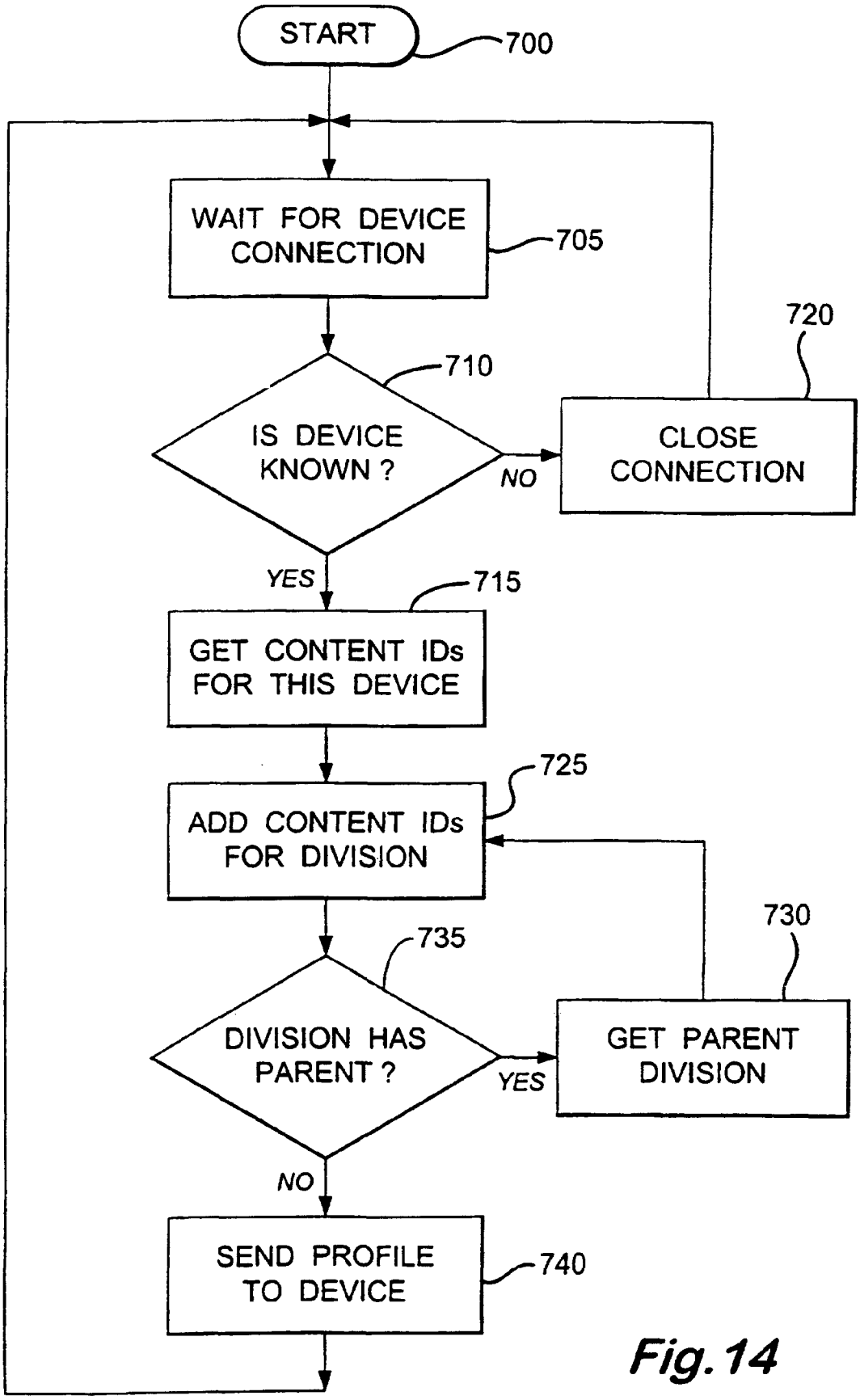

START
700
WAIT FOR DEVICE CONNECTION
705
IS DEVICE KNOWN ?
710
NO
CLOSE CONNECTION
720
YES
GET CONTENT IDs FOR THIS DEVICE
715
ADD CONTENT IDs FOR DIVISION
725
DIVISION HAS PARENT ?
735
YES
GET PARENT DIVISION
730
NO
SEND PROFILE TO DEVICE
740

Fig. 14